Municipalidad de Rafaela
2026

Decreto Firma Conjunta

Número: DFC-2026-196-E-MUNIRAFSF-INT

RAFAELA, SANTA FE
Miércoles 18 de Febrero de 2026

Referencia: LICITACIÓN PÚBLICA. 2do. llamado para la contratación de un Servicio de Software para la Gestión de Alarmas Comunitarias

---

VISTO: Las actuaciones obrantes en el Expediente Letra S - N.º 323.349/1- Fichero N.º 81; y

CONSIDERANDO: Que mediante Decreto N° 57.809 se llamó a Licitación Pública para la contratación de un Servicio de Software para la Gestión de Alarmas Comunitarias.

Que en el acto de apertura, llevado a el día 08 de Septiembre de 2025 se presentó una oferta correspondiendo a la Firma SCARAFÍA GASTÓN MAURO.

Que de la evaluación de los requisitos formales realizada surge que la oferta cumplimenta con la totalidad de los mismos.

Que del informe técnico realizado por la Secretaría de Prevención y Seguridad, surge que la propuesta da cumplimiento a lo solicitado en el pliego de especificaciones técnicas.

Que del informe económico surge que el monto total a adjudicar resulta excesivamente mayor al Presupuesto Oficial por lo que la oferta no es conveniente a los intereses municipales.

Que es necesario realizar un nuevo llamado a Licitación ya que persiste la necesidad de contratación del servicio.

Por ello, el **INTENDENTE MUNICIPAL DE LA CIUDAD DE RAFAELA**

D E C R E T A

Art. 1.º).- Recházase la oferta de SCARAFÍA GASTÓN MAURO con domicilio en calle *Las Magnolias N.º 2159 de la ciudad de Rafaela Provincia de Santa Fe*, por no ser conveniente a los intereses municipales, de acuerdo a lo establecido en el artículo 35.º de la Ordenanza N.º 2.026.

Art. 2.º).- Declárese fracasada la Licitación Pública ordenada por Decreto N.º 57.809.

Art. 3.°).- Apruébase el Pliego General de Bases y Condiciones y el Pliego de Especificaciones Técnicas que como Anexos I y II , respectivamente, forman parte del presente Decreto.

Art. 4.°).- Llámase nuevamente a Licitación Pública para la contratación de un Servicio de Software para la Gestión de Alarmas Comunitarias, la que se regirá por el presente Decreto y sus Anexos, y subsidiariamente, por la Ordenanza Municipal N.º 2.026; el Decreto-Ordenanza Municipal N.º 3.090 y demás legislación municipal vigente que resulte de aplicación.

Art. 5.°).- **PRESUPUESTO, SELLADO Y PLIEGO:**

a) El Presupuesto Oficial asciende a la suma de *Pesos Noventa y Ocho Millones Setecientos Siete Mil ($ 98.707.000.-).*

b) El Sellado Municipal asciende a la suma de *Pesos Cuarenta y Nueve Mil Trescientos Cincuenta y Tres con Cincuenta Centavos ($ 49.353,50.-).*

c) El valor del Pliego se fija en la suma de *Pesos Cuarenta y Nueve Mil Trescientos Cincuenta y Tres con Cincuenta Centavos ($ 49.353,50.-).*

Los pliegos deberán adquirirse en la Dirección de Compras de la Municipalidad de Rafaela, sita en calle Moreno N.° 8 -2.º piso- de esta ciudad de Rafaela, en días hábiles municipales y hasta el día y hora fijados para la apertura de los sobres.

Art. 6.°).- **PROPUESTAS**: Las propuestas deberán presentarse en la Dirección de Compras de la Municipalidad de Rafaela, en sobre cerrado, con la siguiente inscripción: "MUNICIPALIDAD DE RAFAELA - Moreno N.° 8 -2.° Piso- (2300) Rafaela (Provincia de Santa Fe) - Licitación Pública Decreto "Servicio de Software para la Gestión de Alarmas Comunitarias", las que podrán ser presentadas hasta el día y hora fijados para la apertura de sobres y sin ninguna inscripción que permita identificar al oferente.

Art. 7.°).- APERTURA DE LAS PROPUESTAS: Las propuestas se abrirán en dependencias de la Secretaría de Hacienda y Finanza **el día 17 de marzo de 2026, a las nueve (9) horas** o el día inmediato posterior a la misma hora, si aquel resultare feriado, asueto o no laborable para la Administración Pública Municipal.

Art. 8.°).- MANTENIMIENTO DE LAS OFERTAS: Las propuestas deberán mantenerse por un plazo de sesenta (60) días corridos contados a partir del día siguiente al del acto de apertura de las ofertas.

Art. 9.°).- El gasto que demande el cumplimiento del presente se imputará en: B.5.1.4.1.20.35.1/5 - Retribución de Servicios Privados y al Programa de Alarmas Comunitarias de la Secretaría de Prevención y Seguridad y con cargo a ejercicios siguientes.

Art. 10.°).- El presente será refrendado por el Señor Secretario de Prevención y Seguridad y por la Señora Secretaria de Hacienda y Finanzas.

Art. 11.°).- Regístrese, comuníquese, notifíquese, publíquese y archívese.

A N E X O I

PLIEGO GENERAL DE BASES Y CONDICIONES

PARA LICITAR EL SERVICIO DE SOFTWARE PARA LA GESTION DE ALARMAS COMUNITARIAS

Art. 1.°).- OBJETO DE LA LICITACIÓN: El presente pliego establece las bases y condiciones del llamado a Licitación Pública para la contratación del Servicio de Software para la Gestión de Alarmas Comunitarias.

Art. 2.°).- CONOCIMIENTO DE ANTECEDENTES: Quienes concurran a esta licitación no podrán alegar en caso alguno falta de conocimiento del legajo, así como tampoco de las normas legales que regulan el proceso licitatorio. La sola presentación de la oferta significará la aceptación de todas las condiciones fijadas por los mismos.

Las dudas que pudieran plantearse deberán consultarse por escrito, solicitando en forma concreta las aclaraciones que se estimen necesarias.

Art. 3.°).- ELEMENTOS QUE CONSTITUYEN EL LEGAJO: Constituyen este legajo y formarán parte del contrato respectivo, los siguientes documentos:

a) Decreto de llamado a licitación.

b) Pliego General de Bases y Condiciones (Anexo I).

c) Pliego de Especificaciones Técnicas (Anexo II).

d) Posibles aclaraciones posteriores.

Art. 4.°).- CONSULTAS. DOMICILIO ELECTRÓNICO: Las dudas que pudieran plantearse vinculadas a aspectos generales del llamado podrán consultarse por escrito o por e-mail, ante la Dirección de Compras - e-mail: concursodeprecios@rafaela.gob.ar, o en caso de tratarse de dudas de orden técnico ante el Departamento de Tecnología y Comunicaciones e-mail: fferrer@rafaela.gob.ar, ambas de la Municipalidad de Rafaela, solicitando en forma concreta las aclaraciones que se estimen necesarias.

A efectos de poder efectuar consultas por e-mail, los proponentes deberán denunciar una dirección de e-mail que se tendrá como domicilio electrónico constituido a los efectos del proceso licitatorio. Las respuestas y comunicaciones remitidas por la Administración al domicilio electrónico denunciado, se tendrán por válidas aún cuando el proponente no acuse recibo de las mismas, considerándose como fecha de notificación a los fines del cómputo de plazos la de la remisión del e-mail respectivo.

Art. 5.°).- OFERTAS: Las ofertas para la presente licitación deberán presentarse en la Dirección de Compras de esta Municipalidad (calle Moreno N.° 8 - 2.° Piso - Rafaela), hasta el día y hora fijados para la apertura, en sobre cerrado, con la siguiente inscripción: "MUNICIPALIDAD DE RAFAELA - Dirección de Compras - calle Moreno N.° 8 (2.° Piso) - 2300 - RAFAELA (Sta. Fe) - LICITACIÓN PÚBLICA DECRETO **- S**ervicio de Software para la Gestión de Alarmas Comunitarias".

Serán rechazadas y no serán abiertas aquellas ofertas que lleguen con posterioridad al día y hora fijados para la apertura, incluidas las que lleguen por correo o cualquier otro medio, aún cuando se pruebe que fueron despachadas con anterioridad.

Art. 6.°).- FORMA DE PRESENTACIÓN DE LAS OFERTAS Y DOCUMENTOS QUE SE DEBEN ACOMPAÑAR: Los oferentes deberán presentar junto con sus ofertas la siguiente documentación:

a) Recibos o comprobantes oficiales, en original, que acrediten el pago de Pliego.

b) Recibos o comprobantes oficiales, en original, que acrediten el pago del Sellado Municipal

c) Nombres, apellidos o razón social del oferente.

d) La garantía de mantenimiento de la oferta por un importe del 1% del presupuesto oficial. Dicha garantía deberá constituirse en alguna de las siguientes formas:

i. Efectivo, mediante depósito en garantía en la sucursal Rafaela del Nuevo banco Santa Fe S.A., a favor de la Municipalidad de Rafaela.

ii. Pagaré a la vista sin protesto librado por el oferente a la orden de la Municipalidad de Rafaela, con el correspondiente pago del Impuesto del Sellos, abonado en el Banco de Santa Fe S.A.

iii. Póliza de seguro de caución en original, extendida por compañía de Seguro reconocida por la Superintendencia de Seguros de la Nación.

e) Denunciar domicilio real.

f) Constituir domicilio legal en la ciudad de Rafaela.

g) Si fuere una sociedad legalmente constituida, se acompañará fotocopia del contrato social original debidamente inscrito en los registros respectivos, certificada por

autoridad judicial o notarial.

h) Las declaración expresa que el oferente se obliga a cumplir con las disposiciones del presente Pliego, del Decreto de llamado a licitación y de toda otra norma que rija el acto licitatorio.

i) La aceptación expresa del sometimiento a la jurisdicción de los Tribunales Ordinarios de la ciudad de Rafaela, para cualquier cuestión judicial que se plantee con motivo de la contratación, renunciando expresamente a cualquier otro fuero o jurisdicción que pudiere corresponder, inclusive el Federal.

j) El comprobante de inscripción en el Registro de Proveedores de la Municipalidad de Rafaela. Si el oferente no estuviere inscrito, se procederá de acuerdo a lo previsto por el artículo 8.°, segundo y tercer apartado de la Ordenanza N.º 2.026.

k) Debido a que se trata de un nuevo Sistema Informático de Gestión de Alarmas Comunitarias será de suma importancia que cualquier tipo de hardware pueda conectase al software que cuente la Municipalidad de Rafaela al momento de la instalación del software y durante el primer año de implementación del sistema.

l) La propuesta económica, firmada en todas las hojas por el proponente, con aclaración de su apellido/s y nombre/s, según lo establecido en el artículo 8.° del presente.

m) La presentación del pliego firmado en cada una de sus hojas por el oferente.

n) Certificado de libre deuda de Tributos Municipales, extendido por la Oficina de Libre Deuda de la Municipalidad de Rafaela.

ñ) Certificado de libre deuda de multas de tránsito en la Municipalidad de Rafaela, expedido por los Juzgados Municipales de Faltas de Rafaela.

o) Constancia de Inscripción en Oficina Virtual Comercial (ex carpeta empresa).

p) Declaración expresa con carácter de Declaración Jurada manifestando no encontrarse en ningún proceso concursal, ni falencial, ni inhibido, ni inhabilitado para disponer de sus bienes.

Si el oferente fuera una persona jurídica, se deberá adjuntar fotocopia de la documentación que acredite que el firmante tiene facultades suficientes para realizar actos de administración y/o disposición en nombre del oferente, certificada por escribano público o autoridad judicial.

Art. 7.°).- OMISIÓN DE LA DOCUMENTACIÓN: Las propuestas que se presenten sin acreditar el cumplimiento de los incisos a), b), c), d), k) y l) del artículo 6.° serán rechazadas en el mismo momento del acto de apertura de ofertas.

El incumplimiento de los demás requisitos mencionados en el artículo 6.° podrán ser subsanados dentro del plazo de cinco (5) días corridos desde la fecha en que se notifique al oferente. Transcurrido dicho plazo sin que la omisión haya sido subsanada, la propuesta será rechazada.

Art. 8.°).- ESPECIFICACIONES DE LA OFERTA: Las propuestas deberán especificar:

a) Detalle de las opciones a ofertar:

i. El sistema (SOFTWARE) deberá cumplimentar con los 7 ítems especificados en el ANEXO II. De contar con otras funcionalidades, no descriptas, sera importante aclararlas.

ii. Se deberá aclarar específicamente que el software es compatible 100% con todo tipo de hardware existente a la fecha de la instalación del sistema.

b) La cotización deberá incluir todos los impuestos, tributos y gravámenes que el proponente deba afrontar por el ejercicio de la actividad objeto de la licitación, así como también todos los gastos de fletes, instalación y puesta en funcionamiento, en caso que sea necesario.

c) El oferente cotizará de acuerdo a las formas de pago que se especifican en el artículo 26.° del presente pliego.

d) Los oferentes podrán cotizar todas las alternativas que crean convenientes, indicando bajo la palabra ALTERNATIVA a cada una de las distintas opciones.

Art. 9.°).- INVARIABILIDAD DE LOS PRECIOS:

Los precios que consten en las ofertas, y en su caso, los intereses expresados en las mismas, serán invariables por los primeros seis (6) meses calendarios desde la iniciación del servicio; no admitiéndose el reajuste de precios e intereses. Para los meses posteriores se reajustará el valor mensual semestralmente considerando la variación del Indice de Precios al Consumidor (IPC) elaborado por el INDEC.

Art. 10.°).- PRESUPUESTO OFICIAL: El Presupuesto Oficial para el Servicio de Software para la Gestión de Alarmas Comunitarias objeto de la presente licitación asciende a la suma de *Pesos Noventa y Ocho Millones Setecientos Siete Mil ($ 98.707.000.-)*, por el servicio de veinticuatro (24) meses, teniendo la opción de renovación por dos (2) períodos más de un (1) año cada uno.

Art. 11.°).- MANTENIMIENTO DE LAS OFERTAS: Las propuestas deberán mantenerse por un plazo de sesenta (60) días corridos contados a partir del día siguiente al del acto de apertura de las ofertas.

Art. 12.°).- APERTURA DE LAS PROPUESTAS: Las ofertas se abrirán en dependencias de la Secretaría de Hacienda de la Municipalidad de Rafaela (calle Moreno N.º 8 - 2° Piso - 2300 - Rafaela), **el día 17 de marzo de 2026, a las nueve (9) horas**, o el día hábil inmediato posterior a la misma hora si aquel resultare feriado o no laborable para la Administración Pública Municipal.

Los sobres se contarán y enumerarán correlativamente. La apertura se hará siguiendo el orden de numeración que resulte.

Podrán estar presentes todos los interesados y cuanta persona desee asistir al acto. No se admitirán discusiones y los proponentes o sus representantes, únicamente podrán formular observaciones al acto de apertura o a las ofertas, en forma concreta y verbal y ajustadas estrictamente a los hechos-documentos vinculados con el acto de apertura.

Las personas que invoquen representación deberán acreditarla mediante poderes otorgados en legal forma.

Art. 13.°).- ACTA: De todo lo actuado en el acto de apertura, se labrará un acta donde se asentarán las observaciones que formulen los asistentes y las resoluciones de las autoridades municipales que dirigirán el acto.

Dicha acta será firmada por las autoridades municipales que concurran al acto y por los oferentes y asistentes que deseen hacerlo.

En el acta podrán consignarse, según lo dispongan los funcionarios municipales intervinientes, los precios cotizados, así como incluirse como parte de la misma, fotocopias de las ofertas.

Art. 14.°).- IMPUGNACIÓN: Todos los presentes tendrán derecho a impugnar el acto de apertura o cualquiera de las propuestas dentro del plazo de cuatro (4) días corridos de efectuado.

Las impugnaciones deberán ser fundadas y por escrito y serán resueltas, sin substanciación, juntamente con la adjudicación.

Si el acto de apertura tuviera vicios o en él se hubieran violado las disposiciones de algunos de los documentos que rigen el acto licitatorio, el Departamento Ejecutivo Municipal podrá declarar nula la licitación, sin derecho a reclamo alguno por parte de los proponentes.

Art. 15.°).- SELECCIÓN DE OFERTAS: La Municipalidad determinará la conveniencia de aceptar o rechazar las propuestas presentadas, pudiendo declarar fracasada la licitación, sin que ello de derecho a reclamo alguno por parte de los oferentes.

No necesariamente se adjudicará la adquisición del ítem que se licita a quienes ofrezcan el menor precio. La Municipalidad podrá conectar la circunstancia del menor precio con otras como por ejemplo: menor plazo de puesta en marcha el servicio, mayor cantidad de servicios preventivo/correctivo, período de cambio de equipos alquilados, y todo otro criterio cuantitativo o cualitativo que permita la elección de la oferta más conveniente entre aquellas que se ajusten a las bases y condiciones de esta licitación.

Art. 16.°).- OFERTAS IGUALES: Cuando exista igualdad de condiciones entre dos o más ofertas, se procederá de acuerdo a lo establecido en la Ordenanza N.º 2.026 y sus modificatorias.

Art. 17.°).- ADJUDICACIÓN: El oferente al que se le adjudique la presente licitación, deberá presentarse en la Municipalidad de Rafaela, dentro de los diez (10) días de notificado el decreto respectivo, a suscribir el contrato correspondiente, bajo apercibimientos de disponerse la anulación de la adjudicación, sin perjuicio del derecho de este municipio para promover contra el adjudicatario las acciones que jurídicamente correspondan para resarcirse de los daños sufridos.

En caso que se decidiera la rescisión del contrato y revocación de la adjudicación por culpa del adjudicatario, éste deberá dejar de proveer los accesos correspondientes a los equipos que el municipio disponga.

Art. 18.°).- GARANTÍA DE ADJUDICACIÓN: El adjudicatario deberá constituir, dentro de los diez (10) días de notificada la adjudicación, como requisito previo e indispensable para la firma del contrato, una garantía de adjudicación por un monto equivalente al cinco (5 %) por ciento de la oferta adjudicada.

Esta garantía deberá ser instrumentada mediante alguna de las formas previstas para la garantía de mantenimiento de oferta.

Art. 19.°).- DEFECTOS DE FORMA: No serán desestimadas las ofertas que contengan errores de forma u otras imperfecciones que no impidan su exacta comparación con las demás presentadas.

Art. 20.°).- RECHAZO DE LA OFERTA: Además de las causales previstas especialmente en el presente Decreto, será de aplicación el artículo 28.° de la Ordenanza N.° 2.026 según (t.o. con Ordenanza N.° 2.488).

Art. 21.°).- TRANSFERENCIA: El contrato no podrá ser transferido ni cedido por parte del adjudicatario, ni asociarse éste último para su cumplimiento, sin la previa autorización expresa de la Municipalidad de Rafaela.

En caso contrario, la Municipalidad podrá rescindir el contrato, sin recurso por parte del adjudicatario, para exigir el cumplimiento del mismo, aplicándosele al adjudicatario una multa equivalente al cinco (5 %) por ciento del valor adjudicado.

Art. 22.°).- OFERTAS QUE SE APARTEN DE LAS BASES DE LA LICITACIÓN: Las ofertas que se aparten de las bases de la licitación serán desestimadas.

Art. 23.º).- RESCISIÓN POR INCUMPLIMIENTO: Vencido el plazo de entrega del sistema informático sin que ésta se hubiese concretado, el contrato quedará rescindido de pleno derecho, sin necesidad de intimación o interpelación judicial o extrajudicial, debiendo dictar el Departamento Ejecutivo el decreto de revocación.

Art. 24.°).- FALLECIMIENTO O QUIEBRA DEL ADJUDICATARIO: En caso de fallecimiento o quiebra del adjudicatario la Municipalidad podrá, a su exclusivo criterio, y si ello resultara conveniente a los intereses municipales, rescindir el contrato sin otro trámite que la notificación fehaciente a los herederos o al síndico.

Art. 25.°).- PENALIDADES Y MULTAS: Si el contrato se rescindiera por alguna de las causales previstas en este pliego, el adjudicatario perderá la garantía de adjudicación.

Sin perjuicio de lo dispuesto en el párrafo anterior, la rescisión del contrato, por cualquier causal de incumplimiento, hará pasible al adjudicatario de la aplicación de multas. El valor de las multas podrá ascender hasta el diez (10 %) por ciento del valor adjudicado.

Art. 26.°).- FORMA DE PAGO: Los oferentes podrán cotizar por las formas de pago que se detallan a continuación:

a) Pago fijo mensual, por mes vencido, dentro de los diez (10) primeros días de cada mes subsiguiente, conforme a la factura debidamente autorizada.

b) Los oferentes podrán proponer otras formas de pago ALTERNATIVAS.

Art. 27.°).- PLAZO Y LUGAR DE ENTREGA: El software deberá estar instalado, configurado y operativo en las instalaciones que el Secretario de Prevención y Seguridad la Municipalidad de Rafaela defina, o en las dependencias de la misma que se indiquen al adjudicatario. El oferente deberá indicar el plazo en que se propone entregar/instalar los equipos y finalizar la instalación, el que en ningún caso podrá ser superior a veinte (20) días corridos contados a partir de la fecha de firma del Contrato.

Art. 28.°).- IMPUESTO AL VALOR AGREGADO: La Municipalidad de Rafaela es un ente público y no realiza actividades gravadas por el Impuesto al valor Agregado, la condición de la misma en dicho impuesto es de sujeto exento.

Art. 29.°).- Para todos los aspectos no contemplados en el presente decreto será de aplicación la Ordenanza Nº 2.026 y sus modificatorias.

A N E X O I I

ESPECIFICACIONES TÉCNICAS

PLIEGO TÉCNICO PARA EL SUMINISTRO DE SOFTWARE DE GESTIÓN DE ALARMAS COMUNITARIAS

1. INTRODUCCIÓN

La Municipalidad de Rafaela, en el marco de su estrategia de seguridad comunitaria, requiere la provisión de un software de gestión de alarmas comunitarias. Este sistema tiene como objetivo la prevención del delito y la generación de alertas vecinales en la ciudad de Rafaela, que cuenta con aproximadamente 120.000 habitantes distribuidos en 45 barrios.

El software debe ser compatible con cualquier hardware de alarmas disponible en el mercado, permitiendo la gestión, monitoreo y operación de alertas generadas por la comunidad de manera eficiente y segura.

2. ALCANCE DEL SISTEMA

El sistema de alarmas comunitarias debe permitir la administración de alertas vecinales, la notificación a los usuarios y la generación de reportes para su análisis. La solución debe estar diseñada para operar a nivel municipal, con capacidad para administrar eventos provenientes de todos los barrios de Rafaela.

3. REQUERIMIENTOS FUNCIONALES

El software debe cumplir con las siguientes funcionalidades:

3.1. Registro y Gestión de Alertas

· Creación, recepción y administración de alertas comunitarias en tiempo real.

· Categorización de alertas según tipología (robo, emergencia médica, vandalismo, incendio, etc.).

· Registro automático de eventos con datos como ubicación, fecha y hora.

· Validación de alertas por parte de operadores o referentes barriales.

· Priorización de alertas según gravedad del evento.

· Visualización de alertas en un mapa interactivo con geolocalización en tiempo real.

3.2. Notificaciones y Comunicación

· Notificaciones automáticas a usuarios registrados y fuerzas de seguridad.

· Envío de alertas mediante múltiples canales: notificaciones push, SMS, correo electrónico, WhatsApp, Telegram.

· Confirmación de recepción de alertas por parte de usuarios o autoridades.

· Configuración personalizada de notificaciones según tipo de usuario y zona de residencia.

3.3. Gestión de Usuarios

· Diferenciación de roles de usuario: Administrador, Vecino, Referente Barrial, Operador de Seguridad y Autoridad Municipal.

· Control de acceso y permisos según el rol asignado.

· Registro y autenticación segura de usuarios mediante credenciales cifradas y autenticación de doble factor (2FA).

· Registro de auditoría de actividades realizadas en el sistema.

3.4. Exportación y Reportes

· Generación de reportes detallados sobre incidencias y tiempos de respuesta.

· Exportación de datos en formatos CSV para integración con otros sistemas municipales.

· Historial de eventos almacenados con filtros avanzados para análisis posterior.

· Automatización de generación de informes periódicos.

4. REQUERIMIENTOS TÉCNICOS

4.1. Compatibilidad con Hardware

El software debe ser compatible con cualquier tipo de hardware de alarmas comunitarias disponible en el mercado, incluyendo:

· Alarmas cableadas e inalámbricas.

· Botones de pánico físicos y virtuales.

· Cámaras de seguridad con capacidad de detección de eventos.

· Sensores de movimiento e incendios conectados a la plataforma.

4.2. Plataforma de Uso

· Aplicación web responsiva compatible con navegadores modernos (Chrome, Firefox, Edge).

· Aplicación móvil para sistemas operativos Android e iOS.

· Compatibilidad con dispositivos de comunicación IoT mediante protocolos MQTT, HTTP y WebSockets.

4.3. Infraestructura y Almacenamiento

· Hospedaje en servidores en la nube de la Municipalidad de Rafaela.

· Base de datos SQL compatible con las tecnologías empleadas por la municipalidad.

· Arquitectura escalable con balanceo de carga y alta disponibilidad.

· Respaldo de datos automatizado con redundancia geográfica.

5. SEGURIDAD Y PROTECCIÓN DE DATOS

· Implementación de protocolos de seguridad para la protección de la información.

· Cifrado de datos en tránsito y en reposo mediante HTTPS/TLS.

· Autenticación segura mediante credenciales cifradas y autenticación de doble factor (2FA).

· Protección contra amenazas como inyección SQL, XSS y CSRF.

· Registro de auditoría para rastrear actividades sospechosas.

· Cumplimiento con normativas locales de protección de datos personales.

6. MANTENIMIENTO Y SOPORTE

El software debe contar con un plan de mantenimiento que incluya:

· Soporte técnico en horario laboral municipal.

· Actualización periódica de seguridad y mejoras en el sistema.

· Documentación detallada para usuarios y administradores.

· Mecanismos de recuperación ante fallos para garantizar la continuidad operativa.

7. REQUISITOS DE ENTREGA

El proveedor deberá entregar:

· Software completamente operativo y configurado en los servidores de la Municipalidad.

· Documentación técnica y manuales de usuario.

· Capacitación para los operadores del sistema (al menos 6 personas)

Ampliaciones de los puntos 3 y 4:

Requerimientos Funcionales (Punto 3)

Registro y Gestión de Alertas:

El sistema deberá permitir el registro de diversos tipos de alertas comunitarias, tales como robo, emergencia médica, vandalismo, incendio, entre otras. Cada alerta ingresada contendrá información detallada, incluyendo fecha y hora del incidente, tipo de suceso, ubicación georreferenciada y datos del usuario que la reporta. Para garantizar la confiabilidad, las alertas registradas deberán validarse dentro del sistema: esto puede incluir confirmación por parte del usuario que la envía o verificación por un operador antes de ser difundida a toda la red. Además, el sistema asignará un nivel de prioridad a cada alerta según su naturaleza y gravedad (por ejemplo, una emergencia médica tendrá mayor prioridad que un caso de vandalismo), de modo que el flujo de notificaciones alertará primero a los responsables o vecinos correspondientes en situaciones críticas. Todas las alertas se integrarán con un módulo de geolocalización y mapeo interactivo, que ubicará visualmente cada incidente en un mapa en tiempo real, facilitando a los usuarios y a las autoridades la identificación rápida del lugar exacto de la emergencia y permitiendo gestionar eficientemente la respuesta.

Notificaciones y Comunicación:

El sistema dispondrá de múltiples canales de comunicación para difundir las alertas de forma inmediata y efectiva. Se enviarán notificaciones push a quienes utilicen la aplicación móvil, así como mensajes de SMS y correo electrónico para asegurar la entrega aun si los usuarios no cuentan con la app abierta o acceso a datos. Adicionalmente, se integrarán plataformas de mensajería populares como WhatsApp y Telegram, utilizando sus APIs oficiales para hacer llegar las alertas a grupos comunitarios o contactos de emergencia designados. Cada notificación incluirá la información esencial de la alerta (tipo, ubicación, hora) y un enlace o detalle para más información. El sistema incorporará mecanismos de confirmación de recepción, de modo que los usuarios o autoridades puedan indicar que han visto la alerta (por ejemplo, mediante un botón de "Confirmar recibido" en la aplicación o respondiendo al mensaje). Estas confirmaciones permitirán llevar un control de qué miembros de la comunidad o operadores están al tanto de cada incidente. Asimismo, habrá opciones de configuración personalizada de notificaciones según el tipo de usuario: por ejemplo, un vecino podrá elegir recibir solo alertas de su barrio o de ciertos tipos (quizás quiera recibir avisos de robo e incendio, pero no todas las alertas médicas), mientras que un operador de seguridad o policía recibirá todas las alertas de alta prioridad en su jurisdicción. Los administradores del sistema podrán ajustar las preferencias de notificación para roles específicos, asegurando que cada quien reciba la información adecuada por los canales correctos.

Gestión de Usuarios:

El sistema contemplará diferentes roles de usuario, cada uno con permisos y accesos definidos de acuerdo a sus responsabilidades. Por ejemplo, se podrán definir roles como Vecino (usuario comunitario estándar que puede generar alertas y recibir notificaciones de su zona), Coordinador o Referente Barrial (vecino con permisos adicionales para administrar alertas de su barrio o validar información), Operador Municipal (personal de seguridad o emergencia que monitorea y atiende todas las alertas entrantes) y Administrador del Sistema (encargado de la configuración global y mantenimiento de la plataforma). Cada rol tendrá permisos claramente delimitados: los vecinos solo podrán ver y crear alertas relacionadas con su área autorizada, los operadores municipales podrán acceder al listado completo de alertas en tiempo real y marcar su estado (en proceso, atendida, falsa alarma, etc.), mientras que los administradores podrán gestionar usuarios, configurar tipos de alertas, zonas geográficas y canales de notificación, entre otras tareas avanzadas. En cuanto a la autenticación y acceso seguro, el sistema deberá implementar un inicio de sesión protegido, por ejemplo mediante usuario y contraseña cifrada, con políticas de contraseña robustas (longitud mínima, uso de caracteres especiales, etc.) y posiblemente autenticación de dos factores (2FA) para roles críticos (como administradores u operadores). Las sesiones de usuario tendrán un tiempo de expiración para prevenir accesos no supervisados en caso de sesiones olvidadas abiertas. El registro de nuevos usuarios en la plataforma incluirá un proceso de validación: los vecinos deberán proporcionar información personal básica (nombre, dirección, teléfono de contacto, email) que podría verificarse mediante un enlace de confirmación enviado al correo electrónico o código SMS al teléfono. Opcionalmente, la plataforma podría requerir la aprobación por parte de un administrador o la corroboración contra una base de datos municipal (por ejemplo, un padrón de vecinos) para asegurarse de que solo personas autorizadas (residentes de la comunidad) tengan acceso al sistema. Toda la actividad relevante de usuarios (registro, inicio/cierre de sesión, generación de alertas, cambios de configuración) quedará registrada en logs de auditoría para seguimiento y seguridad.

Exportación y Reportes:

El sistema ofrecerá herramientas para la generación de informes detallados que permitan analizar el funcionamiento de las alarmas comunitarias y la incidencia de eventos. Los usuarios con permisos adecuados (por ejemplo, autoridades municipales o administradores) podrán generar reportes periódicos que incluyan métricas como número de alertas por tipo (cuántos robos, cuántos incendios en un rango de fechas determinado), tiempos de respuesta promedio de las autoridades, horas de mayor incidencia de eventos, zonas geográficas más afectadas, entre otros datos relevantes. Estos reportes se presentarán de forma clara, posiblemente con gráficos o tablas, y podrán visualizarse en pantalla o descargarse. Además, el sistema deberá permitir la exportación de datos en formatos estándar como CSV (valores separados por comas) para que la información de las alertas pueda ser utilizada fuera de la plataforma. Por ejemplo, un administrador podría exportar el historial completo de alertas de los últimos seis meses para

analizarlas en una hoja de cálculo o cargarlas en otro sistema municipal de inteligencia o estadística. La exportación podría filtrarse por rango de fechas, por tipo de alerta o por zona, según las necesidades del análisis. Esta funcionalidad facilita la integración con otros sistemas municipales: al tener los datos en CSV (u otro formato compatible), se podría importar la información en plataformas de seguridad ciudadana, tableros de control del municipio, o incluso compartirla con fuerzas de seguridad y organismos de emergencia externos. Adicionalmente, se contemplará la posibilidad de generar informes automatizados (por ejemplo, que el sistema envíe un resumen mensual de alertas al correo de las autoridades correspondientes) y mantener un histórico seguro de todos los reportes emitidos para fines de transparencia y mejora continua.

Requerimientos Técnicos (Punto 4)

Compatibilidad con Hardware:

El sistema deberá ser compatible con los dispositivos físicos y digitales involucrados en las alarmas comunitarias. En primer lugar, soportará la interacción con dispositivos móviles (teléfonos inteligentes y tabletas) que usen los vecinos y operadores, asegurando un correcto funcionamiento en modelos Android e iOS modernos. Además, si la solución incluye componentes de hardware especializados como botones de pánico, sirenas, cámaras de seguridad o sensores de movimiento/incendio instalados en la vía pública o en domicilios, el software debe poder integrarse con ellos. Esta integración se logrará mediante protocolos de comunicación estándar adecuados: por ejemplo, dispositivos IoT (Internet de las Cosas) podrían conectarse usando MQTT para el envío ligero y rápido de mensajes de alerta al servidor; también se podría emplear HTTP/HTTPS para llamadas API REST desde dispositivos que lo permitan (por ejemplo, un panel de alarma que reporte eventos a una URL del sistema), o WebSockets para mantener conexiones activas y bidireccionales en caso de requerir actualización en tiempo real (útil para mostrar en la web la activación de una alarma al instante). Si existen sirenas o alarmas físicas en la comunidad, el sistema deberá ser capaz de disparar una señal a esos equipos cuando se confirme una alerta grave (por ejemplo, activando una sirena barrial en caso de robo confirmado), utilizando interfaces estándar (relés controlados por la plataforma, o comandos a controladores específicos). En resumen, se garantizará que la plataforma pueda comunicarse con múltiples tipos de dispositivos – desde smartphones hasta hardware dedicado – siempre mediante protocolos seguros y confiables, asegurando la interoperabilidad entre el software central y los equipos en campo.

Plataformas de Uso:

La solución será multiplataforma, facilitando el acceso de usuarios desde distintos entornos. Para el acceso vía web, el sistema deberá ser compatible con los principales navegadores de escritorio (Chrome, Firefox, Safari, Edge) en sus versiones recientes, asegurando una visualización correcta y una experiencia fluida. La interfaz web será de diseño responsivo, adaptándose también si se abre desde navegadores en dispositivos móviles o pantallas de distintos tamaños. No obstante, dado que muchos usuarios utilizarán teléfonos, se proveerán aplicaciones móviles nativas para Android e iOS, optimizadas para un rendimiento ágil y para aprovechar funcionalidades del dispositivo (como notificaciones push, geolocalización GPS precisa, vibración/sonido al recibir alertas, etc.). Estas aplicaciones deberán ser compatibles con versiones recientes de los sistemas operativos móviles (por ejemplo, Android 8.0 Oreo o superior, iOS 12 o superior, como referencia), y cumplir con las directrices de las tiendas de aplicaciones (Google Play Store y Apple App Store) en cuanto a seguridad y privacidad. En términos de requisitos, las apps móviles necesitarán permisos como acceso a la ubicación (para asociar coordenadas al emitir una alerta o para mostrarle al usuario alertas cercanas), permiso de notificaciones (para recibir las alarmas en tiempo real) y posiblemente acceso a internet móvil o WiFi permanente para comunicarse con el servidor. Asimismo, el sistema estará preparado para su uso en entornos con conectividad limitada: por ejemplo, utilizando notificaciones SMS como respaldo para aquellos usuarios que no tengan smartphones o conexión de datos en cierto momento. En resumen, cualquier usuario – ya sea desde una PC de escritorio, un portátil, un teléfono inteligente o una tableta – podrá acceder al sistema de alarmas comunitarias, ya sea mediante un navegador web o mediante una app dedicada, sin importar el sistema operativo, siempre que cumpla con unos requisitos mínimos razonables de hardware y software.

Infraestructura y Almacenamiento:

La arquitectura del software estará diseñada para ejecutarse en la nube municipal o infraestructura designada por el municipio, garantizando escalabilidad, rendimiento y disponibilidad. Se implementará una arquitectura de varios niveles (multicapa) que separe la lógica de negocio, la presentación (front-end) y la capa de datos. Por ejemplo, podría haber un servidor de aplicaciones o conjunto de microservicios que gestionen las operaciones (registro de alertas, autenticación, envío de notificaciones, etc.), y un servidor de base de datos SQL dedicado para almacenar la información persistente. La base de datos relacional (por ejemplo, PostgreSQL, MySQL o SQL Server, según lo que el municipio disponga) almacenará tablas con los usuarios, roles, alertas registradas, historial de notificaciones, configuraciones del sistema, entre otros datos. Se definirán índices y estructuras eficientes para permitir consultas rápidas, dado que en situaciones de emergencia es crucial acceder a la información sin demoras. En cuanto a escalabilidad, el sistema deberá poder manejar un crecimiento en el número de usuarios y en la cantidad de alertas sin degradar su performance: esto puede implicar la capacidad de añadir más instancias de servidor de aplicaciones detrás de un balanceador de carga para repartir el tráfico, o mejorar la capacidad del servidor de base de datos (escala vertical) o incluso implementar replicación/clustering de base de datos (escala horizontal) para distribuir la carga de consultas. La infraestructura en la nube municipal deberá proporcionar un nivel de disponibilidad alto; idealmente, el servicio de alarmas comunitarias estará disponible 24/7 con un mínimo de tiempo fuera de servicio. Para lograr esto, se pueden emplear mecanismos de redundancia: por ejemplo, servidores en clúster activos/pasivos que entren en funcionamiento si uno falla, almacenamiento redundante para que no se pierdan datos ante fallos de hardware, y copias de seguridad (backups) periódicas de la base de datos en ubicaciones seguras. También se considerará el uso de contenedores (Docker u otros) y orquestación (como Kubernetes) para facilitar el despliegue, la escalabilidad y la portabilidad de la aplicación dentro de la nube municipal. En resumen, la arquitectura técnica estará preparada para soportar alta concurrencia de usuarios, procesamiento en tiempo real de eventos, y para recuperarse rápidamente ante cualquier falla, garantizando la continuidad del servicio de alarmas.

Seguridad y Protección de Datos:

Dado que el sistema maneja información sensible (datos personales de usuarios, ubicaciones de incidentes, etc.), se implementarán rigurosas medidas de seguridad para proteger la confidencialidad, integridad y disponibilidad de los datos. Toda la comunicación entre los clientes (aplicación móvil, navegador web, dispositivos IoT) y el servidor estará cifrada mediante protocolos seguros (HTTPS/TLS), evitando la interceptación de datos (por ejemplo, protegiendo credenciales de usuario y detalles de alertas durante su transmisión). Asimismo, la información crítica almacenada en la base de datos (como contraseñas de usuarios, tokens de sesión o datos personales) será cifrada o almacenada de forma irreversible: las contraseñas se guardarán empleando funciones de hash seguro con sal, y si se almacenan tokens de autenticación o claves de API, se cifrarán con algoritmos robustos. El sistema deberá incluir protocolos de autenticación fuertes: además del mencionado posible 2FA para ciertos usuarios, se usarán tokens de sesión seguros con expiración y renovación adecuada, evitando así usurpaciones de sesión. También se invalidarán automáticamente las sesiones inactivas o tras cierres de sesión para prevenir accesos no autorizados en dispositivos compartidos. En cuanto a la autorización, cada petición dentro de la plataforma verificará los permisos del rol asociado, asegurando que un usuario no pueda acceder o modificar datos para los cuales no tiene permiso (p. ej., un vecino no puede ver alertas de otra zona que no le corresponde, o un operador no puede modificar configuraciones de sistema reservadas al administrador). Se llevarán registros de auditoría de las acciones importantes (como

creación o eliminación de usuarios, cambios en permisos, eliminación manual de alertas, etc.) para poder rastrear actividades sospechosas o indebidas. El sistema será resistente a amenazas comunes de seguridad informática, aplicando buenas prácticas de desarrollo seguro para prevenir inyección SQL, cross-site scripting (XSS), cross-site request forgery (CSRF) y otros tipos de ataques conocidos. Además, la infraestructura de la nube municipal deberá estar protegida por firewalls, y podrían emplearse sistemas de detección de intrusos (IDS/IPS) para monitorear accesos anómalos. Los datos de respaldo (backups) también se cifrarán y almacenarán de forma segura para prevenir filtraciones en caso de accesos no autorizados a las copias. Por último, se cumplirá con las normativas locales de protección de datos personales y privacidad vigentes (por ejemplo, asegurando el consentimiento de los usuarios para almacenar sus datos, y brindando mecanismos para eliminar o anonimizar información personal si el usuario lo solicita, conforme a la ley). En síntesis, la seguridad estará integrada en todos los niveles del sistema – desde la comunicación y el almacenamiento hasta el uso de la aplicación – para proteger la información de la comunidad y mantener la confianza en el sistema de alarmas.

Requerimientos de la Infraestructura técnica del Oferente

El oferente deberá completar la siguiente tabla, detallando el hardware y software específico y complementario que la plataforma propuesta necesita para su óptimo funcionamiento en un entorno que opera 24/7 (en caso del que software lo necesite). Las especificaciones deben diferenciar entre requisitos Mínimos (para entornos de prueba o baja carga) y Recomendados (para asegurar la estabilidad, escalabilidad y rendimiento continuo bajo una operación crítica).

I. Requisitos del Servidor Central (Hardware y Arquitectura Física/Virtual)

Dado que la operación de monitoreo profesional demanda alta disponibilidad (HA) y la plataforma depende de una base de datos transaccional de alto tráfico (como Microsoft SQL Server, en el caso del oferente anterior), se recomienda la Arquitectura Distribuida/Dual (separando las funciones de Bases de Datos y Aplicaciones Web) en el caso que corresponda.

Componente de Hardware	**Requisito Mínimo Funcional**	**Requisito Recomendado (para CM 24/7 y Escalabilidad)**	**Justificación de la Elección (Explicada por el Oferente)**
Arquitectura del Servidor			
Procesador (CPU)			
Memoria RAM (Total)			
Almacenamiento Primario (OS/DB)			
Red			

II. Requisitos de Plataforma Lógica y Dependencias de Software

El Oferente debe especificar el ecosistema de software de base requerido para la instalación y operación continua de su plataforma, detallando las licencias no incluidas en la suscripción ofrecida (ej. sistemas operativos o bases de datos).

III. Hardware Específico y Requisitos del Puesto de Operación.

Esta sección debe detallar el hardware necesario para los módulos especializados (Grabación, GPS, Video en le caso de que se ofrezcan) y para las terminales que utilizan los operadores. En el caso que sean necesarios

Componente Específico	Requisito Mínimo/Específico	Requisito Recomendado (para Operación Profesional)	Justificación de la Necesidad
Terminales de Operación (Puesto de Trabajo)			
Visualización (Pantallas)			
Continuidad Operacional			

Capacitación: se deberá capacitar al personal municipal (6 personas) para el correcto uso del software.

Soporte Técnico: El soporte técnico para salvar dudas o consultas deberá ser prestado en el horario de 7:00 a 19:00 hs., pudiéndose, en caso excepcional prolongarse el horario hasta las 21:00 hs. A través de una línea telefónica y/o sistema de tikets.

Digitally signed by BRAVINO Silvina Alejandra
Date: 2026.02.12 12:15:28 ART
Location: Ciudad Autónoma de Buenos Aires

Silvina Bravino
Secretaria
Secretaría de Hacienda y Finanzas

Digitally signed by MARTINEZ SALIBA Juan Manuel
Date: 2026.02.18 08:26:16 ART
Location: Ciudad Autónoma de Buenos Aires

Juan Manuel Saliba
Secretario
Secretaría de Prevención y Seguridad

Digitally signed by VIOTTI Leonardo Gaston
Date: 2026.02.18 10:36:39 ART
Location: Ciudad Autónoma de Buenos Aires

Leonardo Viotti
Intendente
Intendencia

Digitally signed by GDE Municipalidad de Rafaela
Date: 2026.02.18 10:37:19 -03:00