

REQUERIMIENTOS DEL SISTEMA POLÍTICO "CONNECT"

Software de Gestión de Estructuras Territoriales Políticas

- **Responsable:** LAIT Technology
- **Fecha:** 20 de Noviembre de 2025
- **Versión:** 1.0
- **Stakeholders:** Pedro Javier Jimenez Bahamon, Andres Anaya Isaza

1. VISIÓN DE ALTO NIVEL

1.1 Problema Central

Las campañas políticas pierden el control de sus estructuras territoriales porque no tienen una forma centralizada y eficiente de conectar con votantes, identificar la atribución real (quién reclutó a quién), medir el crecimiento de la red y segmentar la comunicación.

1.2 Solución

CONNECT es una Plataforma de Gestión Política (SaaS) y CRM desarrollado como PWA (Progressive Web App) que opera múltiples campañas simultáneamente. Convierte votantes en una red organizada usando tecnología accesible: WhatsApp como canal principal de comunicación, códigos QR dinámicos y geolocalización híbrida. Integra autenticación omnicanal y validación de identidad para garantizar la integridad del apoyo político.

1.3 Objetivo

Estructurar redes políticas territoriales de forma escalable, medible y eficiente, permitiendo mapear la estructura en tiempo real y generar métricas para decisiones estratégicas.

1.4 Alcance del Sistema y Evolución

- **Fase 1 (MVP - Versión 1.0): Crecimiento y Estructura.**
 - Foco: Registro de usuarios, consolidación de la base de datos, generación de QRs y validación de identidad. (Módulos 1, 2, 3, 4 y 8).
- **Fase 2 (Expansión - Versión 1.1/1.2): Inteligencia y Comunicación.**
 - Foco: Activación de las herramientas de "Inteligencia Electoral" ya especificadas en este documento:
 - **Módulo 5:** Motor de Mensajería (WhatsApp/Twilio) y Billetera.
 - **Módulo 6:** Mapas de Calor Avanzados y Geofencing (Zonificación visual).
 - **Módulo 7:** Dashboards Analíticos Complejos (Curvas de crecimiento, Mapas de densidad).
 - *Nota:* Aunque estas especificaciones están incluidas en este documento, su despliegue en producción puede ser diferido a la segunda iteración del ciclo de desarrollo.
- **Fase 3 (Futura - Versión 2.0): Operación Logística Día D.**
 - Alcance Exclusivo: Asignación de testigos (witness_ids), coordinación de transporte y carga de evidencia E-14 (RF-3.9).
 - *Estado:* Estas funcionalidades **NO** están detalladas funcionalmente en la v1.0, salvo por los placeholders en base de datos para garantizar migración (ver Nota Técnica RF-4.2.G).
 - **Restricción de UI (Visual Sterilization):** Queda estrictamente **PROHIBIDO** mostrar en los Dashboards operativos (Móvil/Desktop) cualquier widget, botón o contador relacionado con: "Reporte de Votos en Urna", "Carga de E-14", "Asignación de Testigos" o "Estado de Transporte". Estos elementos deben estar ocultos tras la bandera featureFlags.enableDayDModule = false para no confundir la gestión de campaña (Fase 1) con la operación electoral (Fase 3).

2. ESTRUCTURA JERÁRQUICA DEL SISTEMA

1. **SOPORTE TÉCNICO (SUPER_ADMIN):** Nivel de acceso exclusivo para el equipo de desarrollo y configuración del sistema. Encargado de la gestión de parámetros globales (system_config), carga de Divipol (Puestos de

- Votación) y auditoría forense de seguridad. No participa en la operación política diaria.
2. **DIRECCIÓN (ADMIN):** Máximo eslabón de la campaña. Define narrativa, estrategia política y controla el presupuesto operativo. Es el propietario de los datos de la campaña.
 3. **COORDINACIÓN (Estratégico - "El Auditor"):** Responsable de la integridad de los datos y la resolución de conflictos. Es el único con permisos para aprobar "Divorcios" (RF-1.12), validar alertas de fraude (RF-1.10) y autorizar reasignaciones masivas dentro de su zona. Opera principalmente desde Desktop/Tablet.
 4. **ENLACES MUNICIPALES (Rol Técnico: LINK) (Táctico - "El Activador"):** Organizan zonas y convocan eventos. Responsable del acompañamiento físico. Su foco no es mover datos, sino **activar personas**. Se encarga de entregar el material impreso (QRs), capacitar a nuevos Multiplicadores y validar que los líderes sean personas reales (Prueba de Vida). Opera 90% desde Móvil (PWA).
 5. **MULTIPLICADORES (M-001, M-002...):** Reclutan activamente, tienen QR propio.
 6. **SEGUIDORES:** Base electoral. Rastreables por el multiplicador que los reclutó.

Matriz Maestra de Definición de Roles (Source of Truth):

- **Mandato para Desarrollo:** Los términos en español ("Enlace", "Líder") son etiquetas de interfaz (UI Labels). Para la lógica de negocio, reglas de seguridad y consultas a base de datos, se deben utilizar estrictamente las constantes en inglés definidas a continuación.

Rol de Negocio (UI)	Rol de Negocio (UI)	Contexto de Datos (Schema)	Alcance Geográfico (Default)
Soporte Técnico	'SUPER_ADMIN'	users.role	Global / Cross-Platform
Dirección	'ADMIN'	users.role	Campaña Completa
Coordinador	'COORDINATOR'	memberships[].role	geoL1 (Departamento / Municipio)
Enlace	'LINK'	memberships[].role	geoL2 (Comuna / Vereda)

Líder / Multiplicador	'MULTIPLIER'	memberships[].role	Rama Descendente (Red Propia)
Seguidor	'FOLLOWER'	memberships[].role	Individual (Sin hijos)

Nota Técnica: Observe que `SUPER_ADMIN` y `ADMIN` son roles de sistema (Colección `users`, ver RF-4.2.A), mientras que `LINK` y `COORDINATOR` son roles contextuales a una campaña (Array `memberships`, ver RF-4.2.A). Un mismo usuario puede ser `LINK` en una campaña y `FOLLOWER` en otra.

Nota de Elasticidad Jerárquica: La estructura anterior describe la cadena de mando máxima posible (Campaña Nacional). Para elecciones locales (Concejo/Edilato), el sistema aplicará automáticamente una "**Compresión de Roles**", inhabilitando niveles superiores (como Coordinadores Regionales) según la configuración maxScopeLevel de la campaña activa, para evitar burocracia innecesaria en equipos pequeños.

3. CONCEPTOS CLAVE

3.1 Multiplicador Persona que decide unirse activamente al equipo político. Recibe un código QR único, acceso al dashboard de su rama y herramientas para compartir.

3.2 Enlace: Rol de liderazgo intermedio (Mando Táctico) encargado de la gestión operativa de un territorio (Municipio/Comuna). Actúa como el nodo conector entre la estrategia (Coordinador) y la ejecución (Multiplicador). En la lógica de negocio y base de datos, este usuario se identifica estrictamente con el rol LINK.

3.3 Seguidor: Ciudadano que ha completado el registro voluntario, aceptando la vinculación exclusiva con la campaña. Representa la **Base Electoral Confirmada**. Recibe información y es contabilizado en las metas de saturación, pero no tiene funciones de liderazgo ni gestión de red. Rastreable por el multiplicador que lo reclutó.

3.4 Código QR Dinámico (Smart QR) Cada multiplicador tiene un QR único (ej: M-001). A diferencia de un QR estático, este apunta a un middleware que permite

cambiar el destino a una URL de Asistencia vinculada a la colección events, un Formulario o WhatsApp sin reimprimir el código físico.

3.5 Geolocalización Híbrida El sistema captura datos duales para dos propósitos:

1. **Campaña:** "Dónde Vive" (Barrio/GPS) para visitas y mapas de calor.
2. **Día D:** "Dónde Vota" (Puesto de Votación) para logística electoral.

4. REQUERIMIENTOS FUNCIONALES (MÓDULOS PRINCIPALES)

4.1 MÓDULO 1: GESTIÓN DE USUARIOS Y REGISTROS

RF-1.1: Registro Omnicanal y Captura de Datos: El sistema debe soportar la captura unificada de datos a través de cuatro (4) métodos de ingreso, manteniendo la lógica de unicidad por Documento de Identidad (ID).

- **Métodos de Ingreso:**

0. **Código OTP:** Validación telefónica vía SMS/WhatsApp.
1. **Social Auth:** Registro mediante proveedores federados (Google, Facebook, Twitter, LinkedIn) usando Firebase Auth o Auth.js.
2. **Escaneo de QR:** Lectura directa del código de un Multiplicador o Campaña.
3. **Formulario Web:** Registro directo con creación de contraseña segura.

- **Datos de Contacto e Identidad (Obligatorios):**

0. Nombre Completo, Género, Fecha de Nacimiento.
1. **Cédula de Ciudadanía** (ID único - Solo mayores de edad).
2. País, Departamento, Municipio y Dirección de Residencia.
3. Correo Electrónico, Contraseña (Hash) y Teléfono.

4. Validación de Edad (Age Gate):

- **Lógica de Cálculo:** Al ingresar la *Fecha de Nacimiento*, el sistema calcula inmediatamente la diferencia contra la *Fecha Actual* del servidor.
- **Regla de Bloqueo (Strict 18+):**
 - **Condición:** Si $(\text{Fecha_Actual} - \text{Fecha_Nacimiento}) < 18$ años.
 - **Acción UI:** Se deshabilita el botón de "Continuar/Registrar" y el campo de fecha muestra un estado de error rojo.
 - **Mensaje de Error:** "*Registro Restringido: La plataforma es exclusiva para ciudadanos mayores de edad habilitados para votar. No procesamos datos de menores.*"
- **Justificación:** Garantizar el cumplimiento técnico de la política de exclusión definida en el **RNF-7**, evitando la recolección accidental de datos que requieren consentimiento de tutores legales.

5. Validación Geográfica:

El sistema validará que la dirección de residencia exista dentro de los límites geográficos dados (País/Departamento/Municipio).

• Atribución de Referido (Híbrido):

0. **Automático:** Si se escanea QR, el código se pre-carga y bloquea.
1. **Manual (Orgánico):** Si entra por formulario/social sin escanear QR:
 - Se habilita el campo opcional referrerCode.
 - **Estado Inicial (Usuario Flotante):** Si el usuario deja el campo referrerCode vacío, se crea el registro con rol de sistema 'NORMAL' y el array memberships vacío.
 - **Acceso Limitado:** Este usuario tiene acceso a la plataforma para completar su perfil (residencia), pero **NO visualiza**

ningún Dashboard de Campaña ni datos políticos hasta que se ejecute un *Evento de Vinculación* (Escanear QR tardío o Adhesión Voluntaria).

- **Datos de Votación (Zonificación):**

0. **Puesto de Votación:** Campo de selección con búsqueda local (Local Searchable Select). Es Opcional.

1. **Protocolo de Excepción (Puesto No Listado):**

- **Problema:** Si el usuario busca su puesto y no aparece en el listado oficial (Divipol cargada por SUPER_ADMIN).
- **Solución (Fallback):** La lista de resultados debe incluir siempre una opción final fija: "**Otro / No aparece en la lista**".
- **Acción UI:** Al seleccionar esta opción, el dropdown se convierte en un campo de texto libre (Input Text).
- **Persistencia:**
 - El campo votingStationId se marca con el valor reservado 'NON_LISTED'.
 - El texto ingresado por el usuario se guarda en un campo auxiliar manualVotingPlaceName.
- **Feedback:** Se muestra un *Warning* (Amarillo) al usuario: "*Has ingresado un puesto manual. Este dato será verificado por el equipo técnico.*" pero **permite guardar** el registro.

2. **Validación:** Se valida que el puesto pertenezca a la geografía electoral del usuario.

3. **Restricción de Integridad (Time-Lock & Late-Fill Exception):** Se mantiene la regla de bloqueo de edición de puesto cuando la fecha entra en el rango de veda (N días antes de la elección), permitiendo la excepción de *Late-Fill* (una única escritura si estaba vacío).

- **Regla General (Autoservicio):** Cuando la fecha actual entra en el rango de bloqueo (definido en user.membership.campaign.settings.election.electionDate),

el sistema **RECHAZA** cualquier modificación del votingStationId solicitada por roles operativos (Enlace, Multiplicador, Seguidor) si el campo ya tiene valor.

- **Excepción de Completitud (Late-Fill):** Si el usuario llega a la veda con el campo vacío (null), se permite una **única escritura**.
 - **Protocolo de Corrección Administrativa (Admin Override):**
 - **Privilegio:** La restricción de tiempo **NO APLICA** para el rol **ADMIN**. El Jefe de Campaña conserva la facultad de editar este campo en cualquier momento para rectificar errores logísticos.
 - **Mecanismo:** En el Dashboard Administrativo, el campo permanece editable, pero al guardar durante la veda, el sistema muestra una advertencia de confirmación: "*Estás modificando logística crítica en periodo de cierre. Esta acción será auditada.*"
 - **Trazabilidad:** Toda edición forzada genera un registro en audit_logs con actionType: 'FORCE_UPDATE_VOTING_STATION', documentando el valor previo, el nuevo y el Admin responsable.
 - **Fuente de Datos:** El sistema consume exclusivamente la colección interna voting_places (RF-4.2.G).
 - **Comportamiento Offline:** Durante la carga inicial o sincronización, la PWA descarga una copia ligera del catálogo voting_places (filtrada por el departamento/municipio del coordinador si aplica) y la almacena en **IndexedDB** para permitir la selección sin conexión a internet.
 - **Restricción:** Se elimina la conexión directa a la API de Google Maps Places para este campo específico. Si el puesto no aparece, se debe marcar una opción de contingencia "Puesto No Listado" para revisión posterior.
- **Mesa:** Dato numérico Opcional.
- **Edición de Perfil (Post-Registro):**

- El usuario puede modificar su dirección y municipio en cualquier momento.
- **Advertencia de Impacto:** Si el sistema detecta que el cambio de municipio implica salir del alcance de sus campañas actuales, debe mostrar un **Modal de Confirmación** antes de guardar: "*Cambiar tu residencia a [Nueva Ciudad] te desvinculará de las campañas locales de [Ciudad Anterior]. ¿Confirmar cambio?*"

- **Protocolo de Edición de Identificadores (ID Mutation Policy):**

- **Inmutabilidad del Usuario (Self-Service Lock):** El campo documentId (Cédula) es estrictamente de **SOLO LECTURA** para el usuario final y los roles operativos (Enlace/Multiplicador) una vez creado el registro. Esto previene el traspaso de cuentas o la suplantación de identidad post-registro.
- **Corrección Administrativa (Admin Override):** Solo el rol **ADMIN** tiene permiso para corregir errores de digitación en este campo a través del Dashboard.
 - **Validación de Colisión (Pre-Update Check):** Antes de aplicar el cambio, el sistema consulta si el *Nuevo ID* ya existe en la base de datos.
 - *Si existe:* Se bloquea la operación con el error: "*Conflicto de Identidad: La cédula [Nuevo ID] ya pertenece al usuario [Nombre del Otro Usuario].*".
 - *Si no existe:* Se ejecuta la actualización y se genera obligatoriamente un registro en audit_logs con actionPerformed: 'ID_CORRECTION', guardando el valor anterior y el nuevo para trazabilidad forense.

- **Filtro de Admisión (Security Blacklist Check):**

- **Verificación Previa:** Antes de crear un nuevo registro, el sistema consulta si el documentId o phone ya existen en la base de datos con el estado fraudStatus: 'PERMANENT_BAN'.

- **Criterio de Rechazo:** Si se encuentra coincidencia, el sistema **bloquea la creación de la cuenta** inmediatamente (HTTP 403 Forbidden).
- **Justificación:** Impide el reingreso de actores maliciosos que fueron expulsados manualmente por el Administrador o automáticamente por el sistema de seguridad.

RF-1.2: Generación de QR para Multiplicadores Generación automática de identificador (M-001) y QR único al crear un multiplicador.

RF-1.3: Política de Atribución y Vinculación a Campaña

Al registrarse mediante QR, el sistema ejecuta la siguiente lógica de vinculación jerárquica y contextual:

• **Regla de Contexto de Campaña:**

- Al escanear un QR (M-XXX), el sistema consulta el perfil del Multiplicador (`recruitedBy`) y determina cuál es su **Instancia Electoral Activa**.
- **Acción:** Se crea automáticamente un objeto en el array `memberships` del nuevo usuario, estableciendo el campo `campaignId` con el ID correspondiente de la colección `political_campaigns` (ej: "alcaldia_neiva_2026"). Esto garantiza que el usuario quede aislado en el "Silo de Datos" correcto desde el segundo cero.

• **Regla de Jurisdicción (Geo-Fence):**

- El sistema valida que la campaña coincida con el lugar de residencia del usuario. *Ejemplo:* Si el usuario vive en "Bogotá", el sistema bloqueará el intento de unirse a una campaña para la "Alcaldía de Medellín".

• **Regla de Exclusividad (Anti-Doble Militancia Horizontal):**

- El sistema impide la duplicidad de apoyos en el mismo nivel electoral. *Ejemplo:* Un usuario no puede tener una vinculación activa con dos candidatos distintos a la Alcaldía de la misma ciudad simultáneamente.

• **Protocolo Multi-Campaña (Militancia Vertical):**

- **Permisividad:** El sistema **PERMITE** que un mismo usuario (UID único) pertenezca a múltiples campañas simultáneamente, siempre que no violen la regla de exclusividad horizontal. *Ejemplo:* Un usuario puede ser "Líder" en la campaña de *Alcaldía* y "Seguidor" en la campaña de *Concejo*.
- **Aislamiento de Datos (Silo Lógico):** Aunque el usuario es el mismo, sus métricas, rol, jerarquía y reclutados son independientes por cada campaignId. El recruitedCount en *Alcaldía* no suma para *Concejo*.
- **Protocolo de Adhesión Voluntaria (Tráfico Orgánico):**
Define el mecanismo para transformar un usuario 'NORMAL' (sin líder) en un 'FOLLOWER' de una campaña específica mediante interacción directa en la interfaz (Botón "Seguir/Unirme" en el Perfil de la Campaña).
 - **Pre-requisito de Residencia (Mandatory Location Check):**
 - El sistema valida que el usuario tenga completos los datos de geoL2 (Municipio) y address (Dirección/Coordenadas).
 - *Bloqueo:* Si faltan datos, se redirige al usuario a "Editar Perfil" con el mensaje: "*Para unirte a esta campaña, necesitamos saber dónde vives para asignarte a tu equipo local.*"
 - **Mecanismo de Auto-Asignación Geográfica (Geo-Routing):**
 - Al confirmar la adhesión, el sistema ejecuta la lógica de **Punto-en-Polígono (Point-in-Polygon)** (ver RF-6.6) usando la ubicación del usuario contra las zonas activas de la campaña seleccionada.
 - **Escenario A (Dentro de Zona):** Si la ubicación cae dentro de una Zona Territorial activa:
 - Se asigna como recruitedBy al **Coordinador/Enlace** responsable de esa zona.
 - El usuario se integra automáticamente a la estructura territorial de dicho líder.
 - **Escenario B (Fuera de Zona / Zona Vacante):** Si no cae en ninguna zona o la zona no tiene líder asignado:
 - Se asigna temporalmente al **ADMIN** (Dirección de Campaña) o a un usuario "Bodega" designado.
 - Se marca con un flag pendingReassignment: true para que sea reubicado manualmente desde el Dashboard Administrativo.

- **Regla de Permanencia (Soft-Lock):** La vinculación persiste indefinidamente por defecto. Si un usuario ya registrado escanea un QR diferente de un multiplicador de una misma campaña:
 - **Bloqueo Inicial:** El sistema impide el cambio automático para prevenir duplicados accidentales.
 - **Vía de Excepción (Disputa):** Se habilita la opción de iniciar un "Protocolo de Movilidad Voluntaria" (ver RF-1.12) si el votante manifiesta explícitamente su deseo de cambiar de liderazgo.
- **Interacción:** Se actualizan datos si es necesario y se registra un evento de "Interacción/Asistencia" en el log del nuevo multiplicador.
- **Regla de Independencia Geográfica (Universalidad):** La capacidad de reclutamiento NO está limitada por la ubicación física del Multiplicador ni por su zona asignada. Un líder de la "Zona A" puede registrar válidamente a un votante que reside en la "Zona B". El sistema prioriza la **Vinculación Relacional** sobre la coincidencia territorial.
- **Principio de Adhesión Implícita (Definition of Supporter):**
 - **Premisa:** Dado que el sistema aplica la *Regla de Exclusividad* (un solo candidato por nivel electoral) y exige un *Registro Activo* (con validación OTP/Social), se establece que todo usuario registrado (**Role: FOLLOWER**) se considera automáticamente como **Intención de Voto Positiva (Voto Fijo)**.
 - **Política de Persistencia Pasiva (No-Expiry Rule):**
 - **Regla de Negocio:** La falta de interacción digital posterior al registro (ej: no abrir la App, no leer correos, lastActive antiguo) **NO** afecta el conteo de las metas territoriales ni el estatus del usuario.
 - **Distinción de Métricas:**
 - Para **Metas de Votos (KPI Político):** El usuario suma indefinidamente (1) mientras su estado sea ACTIVE. Solo deja de sumar si solicita la baja voluntaria (RF-5.7) o el sistema detecta que se mudó fuera de la zona (RF-1.3 Expatriation).
 - Para **Métricas de Uso (KPI Técnico):** La inactividad solo afecta a los reportes de *Engagement* (ej: "Usuarios Activos Mensuales"), pero nunca elimina el registro de la base de datos operativa.

- **Justificación:** El comportamiento electoral es esporádico. Un votante puede apoyar firmemente sin desear interactuar tecnológicamente cada semana. Eliminarlo por "inactividad" sería subestimar el censo real de la campaña.
- **Restricción de Diseño:** No se implementan campos de "Calificación de Voto" (Indeciso/Opositor) en el formulario de registro ni en el perfil. El sistema está diseñado para la **Gestión de la Tropa Propia**, no para el sondeo de población general abierta.
- **Estratificación de la Adhesión (Vote Quality Tiers):** Aunque todos los registros suman a las metas de crecimiento, el sistema clasifica internamente la "Dureza del Voto" en dos niveles para proyecciones realistas del Día D:
 - **Simpatizante Digital (Voto Blando):**
 - *Definición:* Usuario registrado y validado vía OTP (Teléfono), pero cuya identidad legal (Cédula) no ha sido contrastada contra bases oficiales o verificación presencial.
 - *Valor:* Representa "Intención", pero tiene mayor riesgo de volatilidad o abstención.
 - **Voto Fidelizado (Voto Duro):**
 - *Definición:* Usuario con identityValidationStatus: 'VERIFIED'.
 - *Mecanismo de Ascenso:* El estado cambia cuando el usuario completa exitosamente el **RF-1.16 (KYC Externo)** o un Líder certifica su presencia física mediante el **RF-3.11 (Prueba de Vida)**.
 - *Nota sobre Eventos:* La asistencia recurrente (ej: >3 eventos) **NO** cambia el estado automáticamente, pero genera una "Alerta de Oportunidad" al Coordinador para que priorice la validación de ese usuario activo.
- **Protocolo de Movilidad Geográfica (Electoral Expatriation Check):**
 - **Disparador:** Se ejecuta cada vez que un usuario actualiza su ubicación de residencia (Municipio/Departamento) en su perfil (RF-1.1).
 - **Evaluación de Alcance (Scope Re-validation):** El sistema itera sobre todas las membresías activas (memberships) del usuario y valida la nueva ubicación contra el scope definido en la configuración de cada campaña (political_campaigns).
 - **Acción de Salida (Soft-Exit):**
 - **SI** (Nueva Ubicación \notin Alcance de Campaña):

- El estado de la membresía cambia automáticamente a 'ARCHIVED'.
- Se registra la causal: 'OUT_OF_JURISDICTION'.
- Se decrementan los contadores del Líder original (-1 en recruitedCount), ya que ese voto ya no es útil para esa elección específica.
- **Notificación:** El usuario recibe un aviso: "*Al mudarte a [Nueva Ciudad], has dejado de formar parte de la campaña [Nombre Campaña Anterior].*"
- **SI** (Nueva Ubicación ∈ Alcance): La membresía permanece 'ACTIVE'. (Ejemplo: Mudanza entre barrios de la misma ciudad para una elección de Alcaldía, o mudanza entre ciudades para una elección de Senado).
- **Reingreso:** Para unirse a una campaña local en su nueva ciudad, el usuario debe seguir el flujo estándar de registro (Escanear QR de un nuevo líder local o buscar en el catálogo), garantizando la atribución correcta en el nuevo territorio.
- **Acción de Reingreso (Boomerang Protocol):**
Define el comportamiento cuando un usuario previamente marcado como ARCHIVED actualiza su residencia y vuelve a caer dentro del Scope válido de la campaña.
 - **Reactivación de Estatus:** La membresía cambia automáticamente de 'ARCHIVED' a 'ACTIVE'.
 - **Preservación de Antigüedad (Loyalty Logic):**
 - El sistema **NO** sobrescribe la fecha original de vinculación (createdAt). Esto respeta la "militancia histórica" del usuario.
 - El sistema **restaura** la vinculación con el Líder original (recruitedBy), asumiendo que la relación política persiste.
- **Impacto en Métricas:**
 - El contador recruitedCount del Líder se incrementa (+1), recuperando el "voto perdido" anteriormente.
 - Si el usuario desea cambiar de líder al regresar, debe iniciar explícitamente una **Solicitud de Traslado (RF-1.12)**.

- **Notificación:** El Líder recibe una alerta positiva: "*;Buenas noticias! [Nombre] ha regresado a la zona y se ha reactivado en tu equipo.*"

RF-1.4: Protocolo de Ascenso (Autoservicio) Flujo "Self-Service" para convertir exclusivamente Seguidores en Multiplicadores:

- **Mecanismo:** Botón "Quiero Liderar" en el perfil del Seguidor.
- **Ejecución:** Cambia rol a **MULTIPLIER**, genera QR (M-XXX) y desbloquea Dashboard.
- **Jerarquía:** El usuario **conserva su parentId original**. Su nueva red crece debajo del líder que lo reclutó inicialmente.
- **Nota:** La promoción a roles superiores (Enlace/Coordinador) está reservada para el Administrador mediante el **RF-1.15**.

RF-1.5: Protocolo de Herencia de Nodos (Gestión de Bajas y Estructuras) Regla de "No-Orfandad" y Continuidad Operativa. Define el destino de la red descendente cuando un nodo es eliminado o degradado.

A. Baja de Nodos Tácticos (Multiplicadores y Enlaces):

- **Lógica de Flujo Ascendente:** Si el nodo eliminado es un MULTIPLIER o LINK, sus descendientes directos pasan automáticamente al **Líder Inmediato Superior** (el parentId del usuario eliminado).
- **Estado:** Los usuarios transferidos conservan su estatus activo.
- **Notificación:** El nuevo padre recibe una alerta: "*Has heredado la red de [Nombre Eliminado]*".

B. Baja de Nodos Estratégicos (Coordinadores):

- **Riesgo:** Eliminar un Coordinador afecta a múltiples municipios y enlaces simultáneamente.
- **Lógica de "Safety Net" (Red de Seguridad):**

1. La estructura **NO** se reparte automáticamente entre otros coordinadores.

2. Todos los nodos hijos directos (Enlaces Municipales) se reasignan temporalmente al **ADMIN (Dirección de Campaña)**.

- *Nota:* El rol SUPER_ADMIN (Soporte Técnico) queda excluido de esta lógica de herencia para mantener la neutralidad de los datos técnicos.

3. **Marcado de Cuarentena:** Estos enlaces quedan marcados en base de datos con una bandera hierarchyStatus: 'PENDING_REASSIGNMENT'.

4. **Custodia de Activos Territoriales (Polígonos):**

- **Reasignación de Propiedad:** Los documentos en la colección territorial_zones que pertenecían al usuario eliminado actualizan automáticamente su campo coordinatorId al UID del ADMIN.
- **Cambio de Estatus:** Se actualiza el campo zoneStatus (ver RF-4.2H) a 'VACANT'.
- **Objetivo:** Evitar que el mapa tenga "huecos" o referencias rotas. El territorio sigue existiendo en el sistema, pero se marca explícitamente como un área sin liderazgo asignado, priorizando su re-asignación en el Dashboard del Admin.

- **Visualización en Dashboard:** El Admin ve una sección alerta llamada "Estructuras Sin Coordinador" para que pueda asignar manualmente un nuevo líder regional (Coordinador Interino o Definitivo) en bloque.

RF-1.6: Protocolo de Democión y Continuidad de QR (Traffic Forwarding) Define el comportamiento del sistema cuando un MULTIPLIER o LINK es degradado a FOLLOWER (baja voluntaria de liderazgo), garantizando que el material impreso siga siendo útil.

- **Cambio de Rol:** El usuario pierde acceso a su Dashboard y herramientas de gestión. Su rol en BD cambia a FOLLOWER.
- **Migración de Estructura:** Su red actual de seguidores se transfiere automáticamente al nodo superior inmediato (Padre), siguiendo la misma lógica del RF-1.5 (Herencia).

- **Liberación de Responsabilidad Territorial (Zone Detachment):**

- **Condición:** Si el usuario degradado tenía el rol de COORDINATOR y poseía zonas asignadas en la colección territorial_zones.
- **Acción Automática (Trigger):** El sistema detecta el cambio de rol (before.role == 'COORDINATOR' && after.role != 'COORDINATOR') y ejecuta una rutina de saneamiento:
 - **Búsqueda:** Identifica todos los documentos en territorial_zones donde coordinatorId == UID_Usuario.
 - **Revocación:** Actualiza el campo coordinatorId asignándolo temporalmente al ADMIN principal.
 - **Estado de Vacancia:** Cambia el campo zoneStatus a 'VACANT'.
- **Resultado Visual:** La zona aparece inmediatamente en el Dashboard del Admin como "Territorio Sin Asignar" (con trama de rayas o borde rojo), lista para ser entregada a un nuevo líder, evitando que quede "secuestrada" por un usuario sin permisos.

- **Persistencia del QR Impreso (Smart Redirection):**

- **Problema:** El código QR físico (ej: M-001) sigue circulando en calles, aunque el dueño ya no reclute.
- **Solución:** El código M-001 **NO se desactiva**.
- **Lógica de Atribución:** El middleware detecta que el dueño del QR (status: DEMOTED) ya no puede reclutar.
- **Redirección:** El sistema atribuye automáticamente el nuevo registro al **Líder Superior (Padre)** actual del dueño del QR.
- **UX:** Al escanear, el ciudadano ve un mensaje transicional: "*Tu enlace [Nombre Ex-Líder] ahora apoya al equipo de [Nombre Nuevo Líder]. Tu registro será procesado por este último.*"

RF-1.7: Protocolo de Recuperación de Identidad (Cambio de Número)

Mecanismo para restaurar el acceso cuando el usuario pierde el control de su factor de autenticación principal (SIM Card/Celular) y no posee un método de respaldo (Email).

- **Validación Documental (Identity Anchor):**
 - **Principio:** La solicitud de cambio de número NO puede basarse únicamente en la confianza personal.
 - **Requisito:** El Líder Inmediato o Coordinador debe realizar una **Verificación Visual del Documento de Identidad (Cédula Física)**.
 - **Cotejo de Datos:** El número de la cédula física presentada debe coincidir exactamente con el campo documentId almacenado en el perfil del usuario en la base de datos (colección users).
 - **Responsabilidad:** Al solicitar la migración al Admin, el Coordinador asume la responsabilidad de haber validado la titularidad de la cuenta, generándose un registro de auditoría vinculado a su UID.
- **Mecanismo de Escalamiento (Canal Externo Seguro):**
 - **Restricción:** Dado el alto riesgo de suplantación, la solicitud de cambio de número **NO** se gestiona dentro de la aplicación.
 - **Procedimiento:** Una vez el Coordinador ha validado físicamente la cédula (Identity Anchor), debe instruir al **ADMIN** mediante los canales oficiales de comunicación de la campaña (WhatsApp Corporativo / Email Institucional) definidos en system_config.
 - **Traza:** El mensaje externo actúa como la "Orden de Servicio" para que el Admin ejecute el cambio en el Dashboard.
- **Prevención de Bloqueo (Deadlock Prevention):**
 - **Problema:** El usuario ha perdido simultáneamente el dispositivo y la tarjeta SIM (Número Viejo), imposibilitando la recepción de códigos de confirmación (OTP) en el canal original.
 - **Solución (Human 2FA):** El sistema NO envía códigos de validación al número anterior para autorizar este cambio específico.
 - **Sustitución de Factor:** La autorización digital se reemplaza legalmente por la Validación Biométrica/Documental Presencial realizada por el Coordinador (RF-1.7.A). El Coordinador actúa como "Llave Maestra" temporal para romper el ciclo.
- **Migración de Perfil (Admin Tool):**

- El administrador utiliza una función de "Migración de Identidad" en el Dashboard.
- **Acción Dual:** El sistema actualiza el campo phone en la colección users **Y ADEMÁS** actualiza el registro en el **Proveedor de Autenticación (Auth Core)**, invalidando el token de refresco anterior.
- **Resultado:** Cuando el usuario ingresa con el **Nuevo Número**, el sistema detecta la coincidencia en la base de datos y vuelve a vincular el perfil histórico (votos, reclutados, métricas) a la nueva sesión.

RF-1.8: Herramienta de Reasignación Masiva (Bulk Move Tool) Permite a los Administradores y Coordinadores mover bloques completos de usuarios o sub-estructuras de un nodo padre a otro sin necesidad de eliminar al líder original.

- **Selección Flexible:** Permite seleccionar:
 - **Modo Rama Completa:** Mover un Líder (y toda su descendencia) debajo de un nuevo Jefe.
 - **Modo Hojas (Leafs):** Mover solo los seguidores directos de un Líder A hacia un Líder B, dejando al Líder A en su lugar.
- **Validación de Integridad (Loop Prevention):** El sistema debe validar antes de ejecutar que el nodo destino NO sea descendiente del nodo origen (para evitar referencias circulares infinitas: A es jefe de B, y B se vuelve jefe de A).
- **Procesamiento por Lotes (Batch Write):** Debido a los límites de Firestore (500 operaciones por batch), si la reasignación implica más de 500 documentos, el backend debe dividir la operación en múltiples transacciones atómicas secuenciales.
- **Notificación de Cambio:** Tanto el Líder de Origen (si no es el que se mueve) como el Líder de Destino reciben una notificación: "Se ha reorganizado tu estructura. [N] usuarios han sido transferidos."

RF-1.9: Protocolo de Integridad Estructural (Prevención de Ciclos Infinitos)

Mecanismo de validación obligatoria (Server-Side) que impide la corrupción de la jerarquía mediante referencias circulares.

- **Regla de "No-Ancestro":** Ningún usuario puede ser asignado como subordinado de uno de sus propios descendientes.
- **Límite de Profundidad Vertical (Maximum Depth Guardrail):**
 1. **Contexto:** Aunque Firestore permite documentos de hasta 1MB, un array hierarchyPath excesivamente largo degrada el rendimiento de los índices array-contains necesarios para la seguridad (RF-7.6) y aumenta el costo de serialización.

2. **Regla:** Se establece un límite técnico de **20 niveles** de profundidad en la jerarquía (desde el Candidato hasta el último Seguidor).
 3. **Validación (Pre-Write):**
 - En el registro (RF-1.1): IF (leader.hierarchyPath.length >= 20) REJECT "Estructura demasiado profunda".
 - En reasignaciones (RF-1.8): IF (newParent.hierarchyPath.length + branchDepth > 20) REJECT.
 4. **Garantía de Capacidad:** Con 20 niveles, el campo hierarchyPath consume aproximadamente 600 bytes (< 0.1% del límite de 1MB), garantizando que la restricción física de Firestore nunca sea un problema operativo por causa de la jerarquía.
 5. **Garantía de Escalabilidad Horizontal (Unbounded Breadth):**
 - **Distinción Técnica:** A diferencia del límite vertical (20 niveles) impuesto por el tamaño del documento, el sistema **NO** impone límites al crecimiento horizontal (cantidad de hijos o nietos).
 - **Estrategia de Consulta:** Para recuperar la red descendente ("Mi Estructura"), el sistema utiliza obligatoriamente la consulta where('hierarchyPath', 'array-contains', 'UID_LIDER').
 - *Justificación:* Esta consulta utiliza un índice invertido nativo de Firestore que escala independientemente del número de registros.
 - *Prohibición:* Queda estrictamente **PROHIBIDO** implementar la recuperación de árboles mediante recursividad en cliente o el uso de la cláusula IN con listas de IDs de hijos (where('parentId', 'in', [...])), ya que esto rompería con estructuras de más de 30 nodos de ancho.
- **Escenario de Bloqueo:**
 1. El Usuario A es Coordinador.
 2. El Usuario B es un Multiplicador debajo de A (A -> ... -> B).
 3. Error: Se intenta asignar a B como nuevo jefe de A.
 4. Resultado: El sistema rechaza la transacción con el error CIRCULAR_DEPENDENCY_DETECTED.
 - **Alcance:** Esta validación se ejecuta en:
 1. Asignaciones manuales desde el Dashboard.
 2. Procesos de Reasignación Masiva.
 3. Restauración de usuarios eliminados.

RF-1.10: Protocolo de Integridad de Crecimiento (Anti-Fraud Soft Cap)

Mecanismo de detección de anomalías para prevenir la creación de "Granjas de Bots" o perfiles falsos sin frenar el crecimiento legítimo.

• Umbral de Velocidad (Velocity Check):

- **Regla:** Si un Multiplicador registra > 15 usuarios en < 1 hora (promedio de 1 registro cada 4 minutos, humanamente sospechoso).
- **Acción:** El sistema marca automáticamente al Multiplicador con fraudStatus: 'SUSPICIOUS_VELOCITY'.

• Umbral de Volumen (Volume Cap):

- **Regla:** Cuando un Multiplicador alcanza los **200 Seguidores**.
- **Acción:** Se activa una bandera de fraudStatus: 'NEEDS_VERIFICATION'.

• Efecto de la Marca (Soft Lock):

- **Registro: PERMITIDO.** El líder puede seguir registrando personas (no se rechazan votos).
- **Features Avanzados: BLOQUEADO.** Se deshabilita el acceso a 'Exportación de Datos', 'Visualización de Estructura Completa' y 'Envíos de SMS' hasta que un Coordinador revise la lista y haga clic en [VALIDAR LÍDER].

• Notificación: El Coordinador recibe una alerta: "*El Líder [Nombre] ha crecido inusualmente rápido. Por favor, audita su lista (llamada aleatoria a 3 seguidores) para confirmar veracidad.*"

• Visualización al Usuario (UX Diplomática):

- **Estrategia:** El sistema enmascara el estado de sospecha bajo un mensaje de "Control de Calidad" para no desmotivar a líderes legítimos de alto rendimiento.
- **Componente:** Banner superior fijo (Sticky) en el Dashboard, color Amber-100 (Fondo) y Amber-800 (Texto). **No es descartable.**
- **Texto del Mensaje:**

- **Título:** "🚀 ¡Vas volando! Tu crecimiento es impresionante."
- **Cuerpo:** "Por seguridad y transparencia, hemos pausado temporalmente el acceso a **Herramientas de Gestión y Descargas** mientras nuestro equipo valida la calidad de tus nuevos registros. **Puedes seguir registrando personas normalmente.**"

- **Comportamiento de Botones Bloqueados:**

- Si el usuario intenta hacer clic en un botón restringido (ej: '**Exportar Datos**'), el sistema no lanza error, sino que hace scroll suave (smooth scroll) hasta el banner de advertencia y lo agita brevemente (shake animation) para reforzar el mensaje.

- **Protocolo de Resolución y Auditoría (Accountability Loop):**

- **Interacción:** Al pulsar el botón [VALIDAR LÍDER], el sistema **NO** desbloquea al usuario inmediatamente.
- **Modal Obligatorio:** Se despliega una ventana que exige al Coordinador seleccionar el **Criterio de Verificación** utilizado:

- PHONE_VERIFIED: "Realicé llamada y confirmó datos."
- IN_PERSON_VERIFIED: "Lo conozco / Lo visité presencialmente."
- FALSE_POSITIVE: "El patrón de crecimiento es legítimo (Evento masivo)."

- **Acción Atómica:** Al confirmar, el sistema ejecuta simultáneamente:

- Actualización de Estado: users.fraudStatus = 'VERIFIED'.
- Registro de Auditoría: Se inserta un documento en audit_logs vinculando al Coordinador (actorId) con el Líder sospechoso (targetId) y el motivo seleccionado.

RF-1.11: Módulo de Importación Masiva (Legacy Data Migration) Herramienta para la ingestión controlada de bases de datos externas mediante archivos planos (CSV).

- **Restricción de Volumen (Hard Cap) [NUEVO]:**
 - **Límite:** Se establece un tope máximo técnico de **5,000 filas por archivo CSV.**
 - **Justificación Técnica:**
 - Dado que el procesamiento se define como "**Row-by-Row**" para validar duplicados y jerarquías, el tiempo de ejecución crece linealmente.
 - Un archivo superior a 5,000 registros corre el riesgo de exceder el tiempo máximo de ejecución del contenedor en Cloud Run, provocando que la importación se corte a la mitad.
 - **Validación (Client-Side):** El navegador debe contar las líneas del archivo antes de subirlo.
 - **Acción:** Si rows > 5000, el sistema bloquea la subida inmediatamente y alerta: "El archivo excede el límite seguro. Por favor divídalo en bloques de 5,000 registros".
- **Formato Estricto (Schema Validation):**
 - El sistema provee una plantilla descargable (template_import_v1.csv).
 - Validación de Cabeceras: Si las columnas no coinciden exactamente (ej: cedula, nombre, telefono, direccion, codigo_lider), el proceso se aborta.
 - *Nota de Limpieza:* El Administrador es responsable de eliminar registros de Tarjetas de Identidad (TI) del archivo CSV antes de la carga, conforme a la política del **RNF-7**.
- **Requisito Legal de Ingesta (Provenance Lock):**

Mecanismo de responsabilidad demostrada que impide la carga de archivos sin una atribución legal clara.

 - **Interacción UI (Hard Stop):** El botón final **[PROCESAR IMPORTACIÓN]** permanece estrictamente **DESHABILITADO** (Gris/Unclickable) hasta que el Administrador marque manualmente la casilla de verificación legal.

- **Texto de Declaración Juramentada:** Junto al checkbox, se debe mostrar el siguiente texto legal vinculante:
 - *"Declaro bajo gravedad de juramento que la base de datos suministrada tiene un origen lícito y que cuento con la autorización previa de los titulares para su tratamiento con fines políticos. Asumo total responsabilidad legal y exono a la plataforma de cualquier reclamo por violación de Habeas Data derivado de la procedencia de este archivo."*
 - **Auditoría de Origen:** Al confirmar, el sistema genera un registro en audit_logs con actionType: 'DATA_IMPORT_AFFIDAVIT', guardando el nombre del archivo, el Hash del contenido (para probar que ese fue el archivo juramentado) y la IP del Admin.
- **Protocolo de Sanitización y Normalización (Data Hygiene):**
 - **Limpieza de Identificadores (Critical ID Fix):** Antes de la validación de duplicados, el campo documentId (Cédula) se somete a un barrido estricto para eliminar cualquier carácter no numérico (puntos, comas, guiones, espacios).
 - *Objetivo:* Garantizar que 1.111.222 y 1111222 sean detectados matemáticamente como el mismo ciudadano (Integridad RF-1.1).
 - **Estandarización Telefónica:** El campo phone se limpia para conservar solo los últimos 10 dígitos, eliminando prefijos de país (+57) o paréntesis, asegurando la compatibilidad con el motor de mensajería (RF-5.1).
 - **Seguridad contra Inyección (Formula Injection Shield):**
 - **Amenaza:** Archivos maliciosos que contienen fórmulas ejecutables (inician con =, +, -, @) en campos de texto (Nombre/Dirección).
 - **Defensa:** El sistema detecta estos caracteres al inicio de la cadena y los neutraliza anteponiendo un apóstrofe ('') o eliminándolos. Esto protege a los Administradores que

descarguen estos datos posteriormente vía Exportación (RF-4.3).

- **Codificación:** Conversión forzada a UTF-8 para preservar tildes y ñ, evitando la corrupción de nombres (Mojibake) común en conversiones de Excel/CSV.

- **Lógica de Procesamiento (Row-by-Row):**

- **Deduplicación (Skip Existing):** Antes de escribir, se verifica la existencia del documentId. Si existe, la fila se ignora y se reporta en el log de errores ("Fila 4: Cédula ya registrada").
- **Validación de Jerarquía:** El sistema verifica que el codigo_lider (si se provee) exista. Si no, asigna el registro al Admin que realiza la carga o a un nodo "Bodega de Datos" configurado.

- **Estado de los Datos Importados:**

- **Ubicación:** Se marca location.type: 'MANUAL_TEXT' y geoStatus: 'PENDING'. Esto inserta automáticamente los registros en la cola de trabajo del **RF-6.7** para que el sistema intente buscar las coordenadas esa noche.
- **Legal:** Se marca legalVersionAccepted: 'MIGRATED' y whatsappConsent: false (por precaución), a menos que el Admin marque un checkbox de declaración juramentada: "*Certifico que estos usuarios autorizaron el contacto*".

- **Feedback:** Al finalizar, se descarga un "Reporte de Errores" (.txt) indicando qué filas fallaron y por qué.

- **Protocolo de Activación y Notificación (Silencio por Defecto):**

- **Política de Cero Emisiones:** El proceso de importación es estrictamente silencioso. No se envían SMS ni correos automáticos al finalizar la carga.
 - *Justificación Técnica:* Evitar la activación del "Circuit Breaker Financiero" (RF-5.6) por picos de gasto no autorizados (\$200 USD instantáneos superan el límite de \$50/hora).

- **Marcado de Origen:** Todos los registros creados por este método tendrán forzosamente el campo origin: 'CSV_IMPORT' en la colección users.
- **Ruta de Activación:** Para enviar las credenciales de acceso (Links/QR) a estos usuarios, el Administrador debe programar una campaña manual a través del **RF-5.1**, segmentando por la audiencia "Origen: Importados". Esto permite:
 - Validar el presupuesto antes del envío.
 - Firmar digitalmente la excepción de consentimiento (Legal Override).

RF-1.12: Protocolo de Gestión de Disputas y Transferencias Mecanismo formal para procesar cambios de liderazgo iniciados por el subordinado (Bottom-Up).

- **A. Disparador (The Trigger):**

- Ocurre cuando un usuario existente escanea el QR de un **Nuevo Líder**.
- La PWA detecta el conflicto y muestra: "Ya perteneces al equipo de [Líder Actual]. ¿Deseas solicitar un traslado al equipo de [Nuevo Líder]?"

- **B. Creación de la Solicitud:**

- Si el usuario confirma, se crea un documento en la colección transfer_requests.
- **Motivo Obligatorio:** El usuario debe seleccionar una causal de una lista predefinida:
 - "Cambio de domicilio (Mundanza)".
 - "Conflicto personal con el líder anterior".
 - "El líder anterior está inactivo".
 - "Error en el registro inicial".

- **C. Flujo de Aprobación y Escalabilidad (El Juez Jerárquico):**

El sistema asigna dinámicamente al responsable de resolver la disputa

(approverId) basándose en el rango del usuario solicitante, aplicando el **Principio de Competencia Superior**:

- **Nivel Tropa (Standard Escalation):**
 - **Caso:** El solicitante es FOLLOWER o MULTIPLIER.
 - **Juez:** La solicitud aparece en el Dashboard del **COORDINATOR** de la Zona destino.
 - **Justificación:** El Coordinador tiene la autoridad suficiente para mover piezas operativas dentro o hacia su territorio.
- **Nivel Mando (High-Level Escalation):**
 - **Caso:** El solicitante posee un rol jerárquico (LINK o COORDINATOR) y desea cambiar de zona o estructura.
 - **Juez:** La solicitud se escala automáticamente al **ADMIN** (Dirección de Campaña).
 - **Regla de Conflicto de Interés:** Un Coordinador NO puede aprobar ni rechazar la transferencia de sus propios pares ni de sus Enlaces directos (Links), ya que esto implicaría perder recursos clave o redefinir fronteras territoriales estratégicas.
 - **Visualización:** Estas solicitudes aparecen en una bandeja especial del Dashboard Admin: "*Disputas de Alto Nivel*".
- **Acción:** El Juez designado (Coordinador o Admin) tiene dos botones: **[APROBAR TRASLADO]** o **[RECHAZAR]**.

- **D. Resolución:**

- **Si se Aprueba:** El sistema ejecuta una transacción atómica que actualiza el recruitedBy y el hierarchyPath del usuario. Se recalcula la meta del Líder Viejo (-1) y del Nuevo (+1).
- **Definición de Herencia (Política de Anti-Arrastre):** La transferencia bajo este protocolo es de carácter **Individual Estricto**.
 - **Bloqueo de Estructura:** Si el usuario trasladado posee una red descendente (es Multiplicador o Enlace), esta sub-red **NO se mueve con él**.
 - **Destino de la Red:** Los seguidores del usuario transferido permanecen en la estructura original y son reasignados automáticamente al **Líder Viejo** (Lógica de Flujo Ascendente, ver RF-1.5).

- **Justificación:** Prevenir el "Robo de Estructuras" donde la captación de un solo mando medio arrastre masivamente votos sin supervisión administrativa. Para mover ramas completas, el Coordinador debe utilizar obligatoriamente la **Herramienta de Reasignación Masiva (RF-1.8)**.

- **Notificación:** Ambos líderes reciben una alerta: "El usuario [Nombre] ha sido transferido por orden de Coordinación."

RF-1.13: Protocolo de Gestión de Eventos y Asistencia (Geo-Check-in)

- **Creación:** Los Coordinadores pueden crear eventos desde el Dashboard, definiendo un polígono o punto GPS y un radio de validez (Geofence).
- **Redirección (Flujo QR):** Al asignar un Smart QR a un Evento, el middleware (RF-2.2) redirige al usuario a la URL interna: <https://connect.app/events/{eventId}/checkin>.
- **Validación de Presencia (Cliente PWA):**
 1. Al cargar la página, la PWA solicita permiso de GPS.
 2. **Cálculo Local:** Se compara la posición actual del dispositivo vs. las coordenadas del evento (Fórmula Haversine).
 3. **Registro:**
 - **En Zona:** Si la distancia es menor al radio permitido, se crea el documento en event_attendance con isVerified: true y se muestra el mensaje de "Asistencia Exitosa".
 - **Fuera de Zona:** Se permite el registro pero se marca como isVerified: false y se alerta al usuario: "Estás a [X] metros del lugar. Acércate para validar tu asistencia".
- **Constraint:** Un usuario solo puede registrar una asistencia por EventID (índice compuesto único eventId + userId para evitar duplicados).

RF-1.14: Gestión del Divipol y Geocodificación Maestra (Rol Exclusivo: SUPER_ADMIN): Herramienta del Dashboard Administrativo para la ingestión de la Divipol (División Política Administrativa).

- **A. Registro Manual Asistido (Single Entry):**

- **Input:** El **SUPER_ADMIN** ingresa el nombre oficial del Puesto (ej: "Col. Nacional Santa Librada") y la dirección aproximada.
- **Validación Geográfica (Geocoding Check):** El sistema consulta la **Google Maps Places/Geocoding API** en el backend para validar la existencia física del lugar.
- **Confirmación:** El sistema muestra un mapa con el pin sugerido. El **SUPER_ADMIN** confirma o ajusta la ubicación exacta antes de guardar.
- **Persistencia:** Se guarda el documento en voting_places con el nombre oficial y las coordenadas (geopoint) obtenidas de Google.

- **B. Importación y Geocodificación Batch:**

- El **SUPER_ADMIN** carga el archivo oficial de la Registraduría (CSV) para poblar la colección voting_places antes del inicio de la operación.
- **Geocodificación Centralizada:** El servidor procesa las direcciones de los puestos una única vez utilizando la **Google Maps Geocoding API**.
- **Beneficio de Costo:** En lugar de pagar una consulta API cada vez que un votante se registra (Modelo original RF-1.1), se paga solo una vez por puesto al configurar la campaña.

- **C. Validación Visual:**

- El **SUPER_ADMIN** visualiza los pines generados en el mapa y puede ajustarlos manualmente si la API de Google ubicó mal la escuela o el recinto. * Esto asegura que las coordenadas en voting_places sean precisas y verificadas ("Golden Record").

RF-1.15: Gestión de Jerarquía y Nombramientos (Staffing Admin Tool)

Funcionalidad exclusiva del **Dashboard Administrativo** para designar manualmente la estructura de mando (COORDINATOR, LINK) que no puede generarse por autoservicio.

- **Flujo de Nombramiento (Promoción):**

0. **Selección:** El Admin busca un usuario existente (RF-7.6) y selecciona "Editar Rol".

- **Validación de Congruencia Electoral (Scope Check):**

- **Filtrado de Menú:** Al intentar cambiar el rol de un usuario, el sistema consulta campaign.settings.hierarchy.

- Si COORDINATOR.enabled == false, la opción se oculta.

- **Bloqueo de Asignación Territorial:** Si se intenta asignar una Zona (territorial_zones) a un Coordinador, el sistema valida que la geometría de la zona esté contenida dentro del alcance geográfico de la campaña (territorialScope).

- *Ejemplo:* Si la campaña es "Alcaldía" (geoL2), el sistema **rechaza** la asignación de un polígono que represente el "Departamento" (geoL1) completo, forzando a la campaña a operar solo dentro de sus límites legales.

1. **Cambio de Rango:**

- **A LINK (Enlace):** El usuario mantiene su parentId actual (sigue reportando a su Coordinador) pero adquiere permisos de validación táctica (RF-3.11).

- **A COORDINATOR (Estratégico):** El sistema **eleva** al usuario a la raíz de la jerarquía operativa.

- *Acción de Base de Datos:* Se actualiza parentId al UID del Admin/Candidato para evitar subordinación a rangos inferiores.

- **Advertencia de Degradación:** Si el Admin intenta cambiar un usuario de COORDINATOR a un rol inferior (LINK o MULTIPLIER), el sistema debe mostrar un **Modal de Confirmación**:

- *"Atención: Al degradar a este usuario, se le retirarán automáticamente las zonas territoriales que tenga"*

*asignadas y estas quedarán marcadas como VACANTES.
¿Deseas continuar?"*

2. **Seguridad (Disparador RF-8.9):** Al guardar, se activa el protocolo "Security Kill-Switch", cerrando la sesión del usuario para forzar la recarga de sus nuevos permisos en el próximo inicio de sesión.

- **Flujo de Vinculación Territorial (Opcional):**

0. Una vez ascendido, el sistema ofrece un acceso directo ("Deep Link") al **Módulo de Mapas (RF-6.6)** para asignar inmediatamente al nuevo Líder un polígono o zona de responsabilidad (territorial_zones).

RF-1.16: Validación de Identidad Asíncrona (External KYC)

Integración con servicios de terceros (ej. Truora, MetaMap) para validar la cédula contra bases oficiales.

- **Flujo No Bloqueante:** El registro del usuario se completa exitosamente (HTTP 200) independientemente del resultado de la validación. La verificación ocurre en segundo plano.
- **Propiedad de Estado:** Se añade identityValidationStatus en la colección users con valores: PENDING (Defecto), VERIFIED (Exitosa), FAILED (Inconsistencia).
- **Impacto en UX:** Los usuarios no verificados pueden ver recordatorios en el Dashboard para completar su validación (subir foto de cédula si es necesario).

RF-1.17: Gestión de Políticos y Creación de Campañas

Flujo administrativo para la gestión de candidatos y elecciones.

1. **Solicitud de Rol:** Un usuario registrado solicita convertirse en "Administrador de Campaña".
2. **Validación SUPER_ADMIN:** El equipo de soporte técnico valida fuera de línea la autorización del político y aprueba la solicitud.
3. **Perfil del Político:** El Administrador completa el objeto politicalProfile (Hoja de vida, foto oficial).
4. **Creación de Campaña:** Se registra una nueva entidad definiendo:

- **Tipo de Elección:** (Alcaldía, Gobernación, Presidencia, Concejo, Asamblea, Congreso).
- **Identidad Visual (Theming):**
 - 0. Carga de **Logo Institucional** (Se recomienda fondo transparente).
 - 1. Selección de **Color Primario** (Define el color de la barra de navegación, botones principales y bordes activos).
 - 2. Selección de **Color Secundario** (Usado para resaltados y elementos de acento).
- **Identidad Política:** Lema, Eslogan, Propuestas Clave, Partido Político, Número en Tarjetón.
- *Nota:* Un mismo político puede tener múltiples campañas históricas (ej: Congreso 2015 y Presidencia 2026).

5. Protocolo de "Arranque en Frío" (Day Zero Setup Wizard):

Mecanismo de autoservicio obligatorio que se activa la primera vez que un usuario con rol **ADMIN** ingresa al Dashboard de una campaña recién creada.

- **Bloqueo de Navegación:** El menú lateral y las métricas se ocultan. Se presenta un asistente modal de pantalla completa (Stepper) que no se puede cerrar hasta completar la configuración mínima viable.
- **Paso 1: Delimitación del Tablero (Scope Definition):**
 - 0. *Acción:* El Admin confirma el Departamento y Municipio de la elección (pre-cargados desde la solicitud).
 - 1. *Efecto:* El sistema centra el mapa en esta geografía y descarga los límites oficiales (GeoJSON) del municipio para establecer la "Frontera de Operación".
- **Paso 2: La Primera Piedra (Initial Zoning):**
 - 0. *Problema:* Sin zonas, la lógica de auto-asignación (Geo-Routing) fallaría para los primeros registros.

1. *Acción*: El sistema solicita dibujar el "Cuartel General" o la "Zona 1".

2. *Opción Rápida (Recomendada)*: Botón **[USAR TODO EL MUNICIPIO]**.

0. Si se selecciona, el sistema convierte el límite municipal oficial en la primera zona activa: zona_general_01 y se asigna al Admin como responsable temporal.

○ **Paso 3: Red de Seguridad Financiera:**

0. El Admin debe confirmar o ajustar el maxHourlySpendLimit (Límite de Gasto por Hora) para evitar accidentes con el presupuesto inicial.

○ **Paso 4: Ingesta de Equipo (Staffing):**

0. El sistema genera un **Enlace de Invitación de Alto Nivel** (válido por 24h) específico para invitar a los primeros Coordinadores.

1. *Nota*: Este enlace es diferente al QR de captación de votos; otorga permisos para completar el registro como Staff.

○ **Cierre**: Al finalizar, el Dashboard se desbloquea, el mapa muestra la primera zona activa y el sistema está técnicamente listo para recibir el primer voto sin generar errores de consistencia.

4.2 MÓDULO 2: GENERACIÓN Y ARQUITECTURA DE CÓDIGOS QR

RF-2.1: Motor de Generación de QR Nativo Generación interna (`node-qrcode`) Server-Side. Salida Vectorial (SVG) y Raster (PNG) con corrección de error 'H'.

RF-2.2: Arquitectura de Redirección Dinámica (Middleware) URL Impresa Inmutable (`connect.app/go/M-001`). Interceptor Next.js registra el "Scan Event" en Analytics y redirecciona (HTTP 307) al destino activo (Formulario, WhatsApp, Evento).

4.3 MÓDULO 3: FORMULARIO DE REGISTRO (PWA & LEGAL)

RF-3.1: Progressive Web App (PWA) y Estrategia de Instalación

* **Arquitectura Base:** Formulario instalable, optimizado para móviles con Service Workers y Manifiesto standalone.

- **A. Instalación Nativa (Android/Chrome):** Se captura el evento beforeinstallprompt para mostrar un botón personalizado "Instalar App" dentro del menú principal.
- **B. Protocolo de Asistencia iOS (iOS A2HS Guide - NUEVO):**
 - **Detección de Entorno:** El sistema verifica si Device == iOS Y DisplayMode == Browser (No instalado).
 - **Activación UI:** Si se cumple la condición, se despliega un componente visual tipo "**Tooltip Animado**" o "**Bottom Sheet**" en la parte inferior de la pantalla.
 - **Contenido Instruccional:**
 1. Texto: "*Instala CONNECT para trabajar sin internet.*"
 2. Animación: Una flecha o mano señalando el botón "**Compartir**" (ícono cuadrado con flecha) de la barra de Safari.
 3. Instrucción Final: "*Selecciona 'Agregar a Inicio' (+)*".
 - **Persistencia:** El aviso debe ser descartable ("No volver a mostrar") para no obstruir la navegación si el usuario prefiere usar el navegador web.

RF-3.2: Campos, Auditoría Legal y Compliance Meta

- **Sección Legal (Habeas Data):** Checkbox **Obligatorio** (Ley 1581 de 2012). Sin esto, no se crea el registro.
- **Consentimiento WhatsApp (Canal):** Checkbox **Opcional** pero vinculante.
 - *Texto:* "Autorizo recibir noticias en mi WhatsApp".
 - *Default:* False (Desmarcado por defecto para garantizar consentimiento expreso).

- *Efecto:* Si el usuario lo deja vacío, el registro se guarda exitosamente, pero el campo whatsappConsent se graba como false, inhabilitando futuras comunicaciones por este canal.

- **Auditoría:** Se guarda **Timestamp UTC**, IP, User Agent y estado de ambos checkboxes.
- **Nota Legal:** Para efectos de reportes impresos o jurídicos, el sistema exportará la fecha convertida a GMT-5 (Hora Oficial de Colombia), pero mantendrá el UTC en la base de datos para trazabilidad inmutable.

RF-3.5: Estrategia Offline ("Modo Vereda")

- **Persistencia:** Uso de IndexedDB (Firestore Persistence) para guardar registros localmente. Sincronización automática (Background Sync) al recuperar conectividad.
- **Política de Reintentos y Persistencia de Cola (Sync Queue Policy)** El Service Worker gestiona la cola de sincronización (sync_queue) bajo dos estrategias diferenciadas según el tipo de error HTTP retornado por el servidor:
 - **A. Error de Conectividad (5xx, Timeout, Network Error):**
 - **Estrategia:** Backoff Exponencial (Exponential Backoff).
 - **Lógica:**
 - Intento 1: Inmediato.
 - Intento 2: Espera 2 segundos.
 - Intento 3: Espera 5 segundos.
 - Intento 4: Espera 10 segundos.
 - **Límite:** Tras 4 intentos fallidos, la cola entra en estado PAUSED_NETWORK. Se reactiva automáticamente mediante un event listener window.addEventListener('online').
 - **B. Error de Autenticación (401 Unauthorized / 403 Forbidden):**
 - **Problema:** El Token JWT ha caducado mientras el usuario trabajaba offline.
 - **Lógica de Protección:**
 - **Reintento Silencioso (x1):** El sistema intenta usar el RefreshToken para obtener un nuevo acceso sin molestar al usuario.
 - **Fallo Definitivo:** Si el refresh falla, la cola pasa a estado PAUSED_AUTH_REQUIRED.
 - **UX (No Intrusiva):**

- **NO** se cierra la sesión automáticamente (para no perder el formulario a medio llenar).
 - **NO** se borra la cola de IndexedDB (los datos quedan "congelados" localmente).
 - **Acción:** Aparece un indicador visual persistente (Toast/Banner): "*Sesión vencida. Tus datos están guardados. Toca aquí para reconectar.*".
 - **Resolución:** Al tocar, se abre el Modal de Login. Al validar, la cola se dispara automáticamente.
- **C. Protocolo de Saturación de Almacenamiento (Storage Quota Guard):**
- **Objetivo:** Prevenir la corrupción de datos o el borrado automático del navegador (Eviction) cuando el dispositivo se queda sin espacio físico.
 - **Verificación Preventiva (Pre-Flight):** Antes de iniciar un nuevo registro, el sistema consulta `navigator.storage.estimate()`.
 - **Umbral de Advertencia:** Si `quota_usage > 80%`, muestra un toast amarillo: "Poco espacio. Sincroniza pronto".
 - **Umbral Crítico (Hard Stop):** Si `available < 10MB`, se bloquea la creación de nuevos registros.
 - **Manejo de Excepción (Write Protection):**
 - Si durante el guardado el navegador retorna `QuotaExceededError` (`DOMEexception`), el sistema aborta la transacción inmediatamente.
 - **Acción UI:** Despliega un Modal Crítico (ver Mockup) instruyendo al usuario a liberar espacio en su teléfono (borrar fotos/videos de WhatsApp) antes de reintentar. Nunca se sobrescriben datos antiguos para hacer espacio.
- **D. Visualización de Cola (Feedback Persistente - Sync Badge):**
- **Ubicación:** Se debe implementar un indicador numérico tipo "Badge" superpuesto en el **Icono de Perfil/Avatar** en la barra de navegación principal (Header).
 - **Lógica de Reactividad:** El componente debe suscribirse a los cambios en la tienda local (IndexedDB / sync_queue) para actualizarse en tiempo real.
 - **Estados:**
 - **Sincronizado (0):** El badge se oculta.

- **Pendiente (> 0):** Muestra el número exacto de registros en cola (ej: un círculo naranja con el número "12").
- **Error de Subida:** Si el último intento de sincronización falló por error no recuperable (ver Punto B), el badge cambia a color **Rojo**.
- **Objetivo:** Proporcionar al usuario de campo una métrica visual inmediata de su "Deuda de Datos", incentivando la búsqueda de señal WiFi o 4G antes de finalizar la jornada para "dejar el contador en cero".
- **Resolución de Conflictos ("First-to-Sync Wins"):**
 - **Regla:** Si llegan dos registros de creación para la misma Cédula (ID) capturados offline por diferentes multiplicadores, el que llegue primero al servidor se convierte en el registro oficial (users).
 - **Manejo del "Perdedor":** El registro subsiguiente NO se descarta silenciosamente. El sistema detecta la duplicidad de ID y desvía automáticamente el payload (datos) a una colección de auditoría llamada sync_conflicts.
 - **Notificación:** El multiplicador "perdedor" recibe una notificación: "Usuario ya registrado por otro líder. Tus datos se han guardado para revisión."
 - **Acción [A] Descartar:** El documento en sync_conflicts cambia de estado a DISCARDED. El sistema envía una notificación push al multiplicador "perdedor" (M-002): "*Tu registro de [Nombre] ya existía en base de datos y fue validado por Coordinación.*"
 - **Acción [B] Sobrescribir (Swap):** Se considera que el registro offline, aunque llegó tarde, tiene datos más veraces (ej: corrección de nombre). El sistema actualiza el documento maestro en users con el attemptedPayload del conflicto y cambia la atribución (recruitedBy) si el Admin lo autoriza.
 - **Acción [C] Merge:** Estrategia de enriquecimiento. Si el registro original no tenía address pero el conflicto sí, el sistema inyecta solo el dato faltante sin cambiar el líder (Atribución).
 - **Tabla de Verdad para Fusión de Datos (Merge Logic Matrix):** En el escenario donde se ejecuta una fusión (automática o manual) entre un registro existente en el Servidor ("Master") y un registro entrante desde Local ("Incoming"), se aplican las siguientes reglas de precedencia para garantizar la integridad referencial y legal:

Campo / Grupo de Datos	Estrategia de Resolución	Lógica (Pseudo-código)	Justificación
documentId (Cédula)	Inmutable	Master.id	Es la llave primaria y el ancla del conflicto. No cambia.
recruitedBy (Líder)	Server Authority (Bloqueo)	Master.recruitedBy	Protege la regla de "Vigencia Eterna" (RF-1.3). El líder original nunca se pierde por una sincronización posterior.
phone / whatsapp	Enrichment + Latest	`Incoming.phone	
location (Coordenadas)	Precision Wins	(Master.type == 'GPS') ? Master : Incoming	Si el servidor ya tiene GPS real, se conserva. Si solo tiene texto manual y llega un GPS, se actualiza.
address (Texto)	Enrichment	Master.address ?? Incoming.address	Solo se llena si el campo en el servidor estaba vacío (null o ""). No sobrescribe direcciones validadas.
whatsappConsent	Restrictive (Legal)	Master.consent && Incoming.consent	Principio de Prudencia: Si alguno de los dos es false (revocación), el resultado final es false para evitar demandas por Spam.
votingStationId	Latest Wins	Incoming.stationId	La zonificación puede cambiar cerca al Día D. Se asume que el dato más fresco es la corrección del puesto.
metadata (Timestamps)	Audit Trail	Merge(Master.meta, Incoming.meta)	Se conserva la fecha de creación original (createdAt), pero se actualiza lastUpdated.

RF-3.6: Sistema de Notificaciones y Feedback (Estados de UI)

Escenario	Tipo	Mensaje / Visual (UX)
Validando Cédula	Spinner	Animación local en input. No bloquea navegación.
Enviando	Bloqueo	Overlay con Spinner. Bloquea doble submit.
Carga Dashboard	Skeleton	Bloques grises pulsantes.
Cédula Duplicada	Info	"Usuario ya registrado. Datos actualizados."
Conflicto Rama	Warning	"El usuario pertenece a [Líder]. Se registra visita."
Offline (Captura)	Estado (Toast)	"Sin señal. Guardando localmente...". No Bloqueante. El usuario sigue trabajando. Icono de nube tachada en esquina.
Offline (Crítico)	Alerta Modal	"Conexión Requerida". Bloqueante. Impide acciones Server-Side estrictas (Recargas, Envíos SMS, Login). Botón "Reintentar" visible.
Token Vencido (Sincronización)	Warning (Naranja)	"Sesión expirada. Datos en pausa." Icono de candado. No bloquea la navegación, pero impide nuevos envíos hasta que el usuario re-autentique manualmente (toque el aviso).
Registro Cross-Zona	Warning (Amarillo)	"¡Registro Exitoso! Nota: El votante vive en [Zona B], fuera de tu territorio"

Escenario	Tipo	Mensaje / Visual (UX)
		asignado. Suma a tu red personal, pero no a tu meta de zona."
Bloqueo de Edición (Puesto)	Icono Candado	El Select de Puesto de Votación aparece deshabilitado (gris) con un <i>tooltip</i> : "Edición cerrada por inminencia electoral. Tu puesto ya está confirmado."
Aviso de Asignación Tardía	Warning (Modal)	Al intentar guardar un puesto vacío durante la veda: "Estás asignando tu puesto a pocos días de la elección. Confirma bien , ya que no podrás cambiarlo después."
Acceso Denegado (Lista Negra)	Error (Modal Crítico)	" Registro No Permitido: Tu identificación cuenta con una restricción administrativa permanente en esta campaña. Si crees que es un error, contacta a tu enlace."

RF-3.7: Experiencia de Aterrizaje (Onboarding & Welcome Kit) Estrategia de "First Time User Experience" (FTUE) para generar conexión emocional inmediata.

A. Modal de Bienvenida (Overlay):

- **Disparador:** Se activa automáticamente cuando la API confirma el registro exitoso (HTTP 200/201).

- **Contenido Multimedia:**

- Se reproduce un video corto (30-45 seg) del Candidato/Líder.
- **Formato:** Embed de YouTube/Vimeo (para no recargar el servidor) o WebM optimizado (< 2MB).

- **Mensaje:** "Gracias por unirte, [Nombre]. Tu apoyo es clave para transformar [Ciudad]."

B. Micro-Instrucciones (Tour Guiado):

- Si el usuario es **Multiplicador**, se le muestra un tutorial de 3 pasos (Carousel):
 1. "Este es tu Código QR".
 2. "Compártelo con tus amigos".
 3. "Mira tú **progreso** en el Dashboard".
- Si el usuario es **Seguidor**, se le invita a unirse al Canal de WhatsApp Oficial (si dio consentimiento).

C. Estrategia de Estado Vacío (Empty State - Activation Mode):

Define la interfaz persistente que ve el usuario *después* del Tour inicial, pero *antes* de tener resultados.

- **Condición de Disparo:** Se activa SI `user.role == 'MULTIPLIER'` y `user.metrics.recruitedCount == 0`.
 1. *Nota:* Los usuarios con rol FOLLOWER no entran en este estado; pasan directamente a la **Vista Seguidor (RF-7.1.3)**.
- **Ocultamiento de Complejidad:** Se esconden los módulos de "Mapas de Calor", "Curvas de Crecimiento" y "Listados de Seguidores" (ya que estarían vacíos).
- **Interfaz de Activación (Action-First UI):** En su lugar, se muestran tres tarjetas de acción grandes (Hero Cards):
 1. **Tu Herramienta:** Visualización central del Código QR (M-XXX) listo para escanear.
 2. **Tu Misión:** "Registra a tu primera persona". Botón primario grande: **[NUEVO REGISTRO]**.
 3. **Tu Meta:** Barra de progreso visual "0 de 1 completado" para gamificar el primer paso.

- **Transición:** En el momento en que el contador sube a 1 (vía Trigger RF-4.5), la interfaz se desbloquea automáticamente y revela el Dashboard Analítico completo con confeti virtual (Micro-interacción de celebración).

D. Gestión de Membresías (My Campaigns):

- Dentro de la vista "Mi Perfil", se habilita un botón o sección llamada "**Mis Campañas**".
- **Interfaz de Lista:** Al acceder, el usuario visualiza una tabla o lista de tarjetas con todas sus vinculaciones activas.
 - *Datos:* Logo de Campaña, Nombre del Candidato, Rol Actual (Líder/Seguidor).
 - *Acciones:* Botón "Ir al Dashboard" (Cambio de contexto) y Botón "Desvincularse" (Abandonar campaña específica).

RF-3.8: Protocolo de Versionado Legal y Re-Consentimiento (The Legal Wall)

Mecanismo de protección jurídica que bloquea la operatividad de la aplicación si los términos cambian sustancialmente en la base de datos, forzando una nueva aceptación expresa.

A. Verificación Continua (Session Resume Check):

- **Disparador:** Cada vez que la PWA se inicia, se recarga o regresa del segundo plano (App Resume), el Middleware ejecuta una validación crítica:
 - IF (user.legalVersionAccepted != system_config.legal.currentTermsVersion)
 - AND (system_config.legal.isMandatoryUpdate == true)
- **Justificación:** Esto asegura que incluso los usuarios con sesión permanente ("Recordarme") sean interceptados inmediatamente tras un cambio de política.

B. Bloqueo de Interfaz (Modal Crítico):

- **Acción de Sistema:** Si se detecta desactualización, el enrutador (Next.js Router) redirige forzosamente a /legal/update-required.

- **Restricción:** Se eliminan los botones de "Cerrar" o "Atrás". El usuario queda en un "callejón sin salida" funcional.
- **Acción Única:** Solo hay dos caminos posibles:

1. Botón [LEER Y ACEPTAR NUEVOS TÉRMINOS]:

- Actualiza users.metadata.legalVersionAccepted a la nueva versión (ej: 'v2.1').
- Registra fecha, hora e IP en audit_logs.
- Desbloquea el acceso al Dashboard.

2. Botón [NO ACEPTO / DARME DE BAJA]: * Dispara inmediatamente el Flujo 5: Derecho al Olvido (Anonimización) y cierra la sesión.

RF-3.9: Protocolo de Carga Resiliente de Evidencia (E-14 Multi-Shot)

[ALCANCE FASE 3 - NO IMPLEMENTAR UI EN v1.0] Mecanismo de subida tolerante a fallos y estrategia de captura segmentada.

- **Nota para QA y Desarrollo:** Este requerimiento define la arquitectura futura. En la versión v1.0, la funcionalidad de carga de testigos NO DEBE ESTAR VISIBLE.
- **Estado en v1.0:**

- **Backend (Storage):** Se configuran los *buckets* de Google Cloud Storage (/e14-evidence).
- **Frontend (UI):** Los botones de "Subir E-14" deben estar ocultos mediante un *Feature Flag* (system_config.featureFlags.enableDayDModule = false).

• Estrategia de Captura UI (User-Guided Tiling) [Reservado Fase 3]:

- **Problema:** Una sola foto de un documento largo (60cm) resulta en números ilegibles o borrosos.
- **Solución:** La interfaz obliga al Testigo a completar una secuencia de 3 pasos:

1. [CAM 1] Foto Encabezado: (Captura zona de Mesa y Municipio).

2. [CAM 2] Foto Votos: (Captura el cuerpo central de candidatos).

3. [CAM 3] Foto Firmas: (Captura jurados y observaciones).

- **Validación:** No se permite enviar el formulario si falta alguno de los segmentos.

- **Arquitectura de Fragmentación (Chunked Uploads) [Reservado Fase 3]:**

* Dado el aumento de tamaño (aprox. 9MB totales por mesa), se mantiene la división en *chunks* de 256 KB para garantizar que la subida no falle en redes 3G inestables.

- **Estándar de Feedback Visual (Non-Blocking UX Strategy) [Reservado Fase 3]:**

- **Restricción de Interfaz:** Queda prohibido el uso de *modales bloqueantes* o *spinners de pantalla completa* durante el proceso de carga de evidencias (E-14), ya que la transmisión fragmentada puede durar minutos en zonas rurales (EDGE/3G).
- **Componente Obligatorio:** Se debe implementar un indicador de progreso no intrusivo tipo "**Global Snackbar**" (Barra inferior persistente) que muestre el avance acumulado de los *chunks* (ej: "Sincronizando Mesa 4: 45%...").
- **Continuidad Operativa:** Este componente permite al usuario seguir navegando o registrando nuevos datos mientras la subida ocurre en segundo plano.
- **Cierre de Ciclo:** Si el navegador lo soporta, el sistema disparará una **Notificación Web Push Local** al completar el 100% de la carga, confirmando la recepción exitosa por el servidor sin necesidad de que el usuario tenga la app abierta.

RF-3.10: Modo de Contingencia Operativa (Safe Mode / Lite Version)

Mecanismo de degradación funcional controlada para situaciones de alta inestabilidad o fallo de servicios externos.

- **Disparador:** Un interruptor global en system_config.featureFlags.emergencyMode (Boolean).

- **Comportamiento "Lite":** Al activarse, la PWA se recarga y aplica las siguientes restricciones para aligerar la carga:
 - 1. Mapas Desactivados:** Se fuerza el comportamiento de "Modo Fallback" (RF-6.5) globalmente. Nadie carga Google Maps.
 - 2. Validaciones Relajadas:** Se desactivan validaciones asíncronas complejas (ej: verificación de antecedentes en tiempo real) para priorizar la velocidad de captura.
 - 3. UI Simplificada:** Se ocultan dashboards, gráficos y animaciones. La interfaz se reduce estrictamente al Formulario de Entrada de Datos.
- **Objetivo:** Garantizar que, incluso si los servicios de terceros (Mapas, Twilio) fallan, la capacidad de registrar votantes y subir E-14 permanezca operativa.

RF-3.11: Protocolo de "Prueba de Vida" (Validación de Enlace)

Funcionalidad exclusiva para el rol LINK y superior.

- **Objetivo:** Certificar que un Multiplicador recién registrado es una persona real y confiable antes de entregarle recursos de campaña.
- **UI:** En el perfil del Multiplicador, el Enlace ve un botón [CERTIFICAR LÍDER].
- **Acción:** Al pulsarlo, el sistema:
 1. Registra la geolocalización actual del Enlace (debe coincidir físicamente con la zona).
 2. Marca al usuario con verificationStatus: 'VERIFIED_IN_PERSON'.
 3. Habilita funcionalidades avanzadas para ese Multiplicador (ej: solicitar **reabastecimiento de kits impresos y publicidad**).

4.4 MÓDULO 4: BASE DE DATOS (FIRESTORE)

RF-4.1: Estrategia de Estructura de Datos (Colecciones Planas) Arquitectura de colecciones raíz con referencias (IDs), evitando subcolecciones anidadas para facilitar consultas globales y reasignación de ramas.

RF-4.2: Esquema JSON Definido

- **Estándar de Temporalidad (Global Timezone Policy):**

- **Persistencia (Backend):** Todos los campos de tipo timestamp (ej: createdAt, lastActive) se almacenan en Firestore estrictamente en formato **UTC (ISO 8601)**.
- **Renderizado (Frontend):** La interfaz de usuario debe convertir estos valores a la zona horaria local del dispositivo del usuario en el momento de la visualización (Client-Side Resolution).
- **Justificación:** Garantiza que un log de auditoría generado a las 23:00 (UTC) no aparezca con fecha del "día siguiente" incorrectamente si se consulta desde otra longitud.

A. Colección users (Usuarios y Jerarquía)

```
{
  "uid": "string (AuthID)",
  "userType": "string ('CITIZEN' | 'POLITICIAN')",
  "role": "string ('SUPER_ADMIN' | 'ADMIN' | 'NORMAL')",
  "identityValidationStatus": "string ('PENDING' | 'VERIFIED' | 'FAILED')",
  "email": "string",
  "passwordHash": "string (Si usa Auth propio, sino gestionado por Provider)",
  "searchKey": "string (Índice Compuesto: fullName + alias. Normalizado: 'maria perez la mona')",
  "profile": {
    "fullName": "string",
    "alias": "string (Opcional - Ej: 'El Profe', 'La Mona')",
    "gender": "string ('M' | 'F' | 'OTHER')",
    "birthDate": "timestamp",
    "documentId": "string (Cédula Indexed Unique)",
    "phone": "string",
    "whatsappLink": "string"
  },
  "politicalProfile": { // Objeto opcional, solo si userType == 'POLITICIAN'
    "bio": "string",
    "photoUrl": "string",
    "partyAffiliation": "string",
    "createdBy": "string (UID del usuario ADMIN)",
  },
  "location": {
    "country": "string",
    "geoL1": "string",
    "geoL2": "string",
    "geoL3": "string | NULL",
    "address": "string", // Dirección validada
    "votingStationId": "string (Ref a 'voting_places' | 'NON_LISTED')",
    "manualVotingPlaceName": "string | NULL",
    "votingPlaceParams": { "table": number }
  },
  "memberships": [
  {
    "campaignId": "string (Ref a political_campaigns)"
  }
]
```

```

    "role": "string ('AUX_ADMIN' | 'COORDINATOR' | 'LINK' | 'MULTIPLIER' |
'FOLLOWER')",
    "recruitedBy": "string (UID del Referidor)",
    "hierarchyPath": ["UID_ADMIN", "UID_Coord", "UID_Link", "UID_Mult"],
    "isCrossZone": "boolean (true si calculatedZoneId !=
parent.assignedZoneId)",
    "calculatedZoneId": "string (Ref a 'territorial_zones' - Autoasignado) |
'UNCATEGORIZED'",
    "manualZoneOverride": "boolean (True si un admin cambió la zona
manualmente)",
    "personalGoal": "number (Opcional. Null)",
    "recruitedCount": "number (Computed | Read-Only)", // Actualizado solo por
Cloud Function
    "status": " string ('ACTIVE' | 'PENDING_REASSIGNMENT' | 'ARCHIVED')"
}
],
"metrics": {
    "lastActive": "timestamp",
    "whatsappConsent": "boolean",
    "consent_evidence": {
        // Requerido para auditoría Meta
        "ip": "string (192.168.x.x)",
        "timestamp": "timestamp (Fecha exacta del Checkbox)",
        "userAgent": "string (Dispositivo/Navegador)",
        "origin": "string ('PWA_REGISTRATION' | 'PAPER_DIGITIZATION' |
'CSV_IMPORT')"
    },
    "fraudStatus": "string ('NORMAL' | 'SUSPICIOUS_VELOCITY' |
'NEEDS_VERIFICATION' | 'VERIFIED')",
    "metadata": {
        "createdAt": "timestamp",
        "legalVersionAccepted": "string (v1.0)",
        "sourceQr": "string (M-001)"
    }
}
}

```

B. Colección messaging_campaigns (Gestión de Mensajería)

```
{
    "id": "string (Auto-ID)",
    "name": "string",
    "politicalCampaignId": "string (Ref a political_campaigns)",
    "status": "string ('DRAFT' | 'SCHEDULED' | 'COMPLETED')",
    "config": {
        "templateSid": "string (Twilio Template ID)",
        "templateName": "string (Ej: 'alerta_cierre_mesa')", // Para referencia
humana
        "templateReviewStatus": "string ('APPROVED' | 'PENDING' | 'REJECTED')",
        "messageType": "string ('MARKETING' | 'UTILITY')",
        "budgetAllocated": "number (USD)",
        "appliedCost": "number (0.04 o 0.08 según segmentos)",
        "segmentCount": "number (Calculado al cierre de edición)"
    },
}
```

```

"segmentation": {
    "targetRoles": ["FOLLOWER"],
    "targetZones": ["Comuna 4", "Zona Norte"],
    "targetOrigin": "string (Opcional, ej: 'CSV_IMPORT')"
    "excludeAlreadyContacted": "boolean"
},
"stats": {
    "sent": "number",
    "delivered": "number",
    "read": "number",
    "replied": "number",
    "responseDistribution": {...}
    "totalCost": "number"
},
"audit": {
    "createdBy": "string (UID)",
    "approvedBy": "string (UID)"
}
}

```

C. Colección audit_logs (Seguridad)

```

{
    "id": "string (Auto-ID)",
    "timestamp": "timestamp",
    "actorId": "string (UID)",
    "actionType": "string ('LOGIN' | 'QR_SCAN' | 'EXPORT_DATA' | 'USER_DELETE' |
    'VIEW_PROFILE' | 'SESSION_REVOKED_LIMIT' | 'SESSION_REVOKED_ROLE_CHANGE' |
    'MANUAL_FRAUD_CLEARANCE')",
    "targetId": "string (UID afectado)",
    "details": {
        "ipAddress": "string",
        "userAgent": "string",
        "changes": { "before": "map", "after": "map" },
        "verificationMethod": "string (Opcional, ej: 'PHONE_VERIFIED')",
        "exportMode": "string ('MASTER' | 'OPERATIVE')", // Campo Crítico
        "queryFilter": "string (Ej: 'Municipio: Neiva')",
        "recordCount": "number",
    }
}

```

D. Colección wallet_transactions (Ledger Financiero)

```

{
    "id": "string (Auto-ID)",
    "type": "string ('DEPOSIT' | 'SPEND' | 'REFUND')",
    "amount": "number (Positivo para DEPOSIT, Negativo para SPEND)",
    "balanceAfter": "number (Snapshot del saldo resultante)",
    "description": "string (Ej: 'Recarga Inicial' o 'Campaña SMS #12')",
    "referenceId": "string (ID Campaña o MessageSid de Twilio)",
    "failureReason": "string (Opcional: código de error Twilio, ej: '30008 - Unknown Error')",
    "adminUser": "string (UID del Admin que autorizó)",
}

```

```

    "timestamp": "timestamp",
    "metadata": {
        "method": "string ('SYSTEM_WEBHOOK')",
        "automated": true,
        "reference": "string (Requerido si type=='DEPOSIT': Nro. Comprobante Bancario o Acta) // [UNIQUE CONSTRAINT] Requerido si type=='DEPOSIT'. No puede repetirse en toda la colección para evitar doble gasto."
    }
}

```

E. Colección system_config (Configuración Global)

```

{
    "id": "v1_settings",
    "platform_financials": {
        "currency": "string ('USD')",
        "costPerMessage": "number (0.04)", // [Writer: SUPER_ADMIN] Tarifa SaaS estándar
        "costPerMessageUtility": "number (0.02)"
    },
    "legal": {
        "currentTermsVersion": "string ('v2.1')", // Versión de Términos de Uso de la APP
        "termsUrl": "string (https://connect.app/terms.pdf)",
        "isMandatoryUpdate": "boolean"
    },
    "featureFlags": {
        "maintenanceMode": "boolean", // Baja el sistema para TODOS
        "allowNewRegistrations": "boolean",
        "emergencyMode": "boolean" // UI Lite global
    },
    "security": {
        "globalWhitelistedIps": ["190.158.xx.xx"] // IPs de Soporte Técnico (LAIT)
    }
}

```

F. Colección sync_conflicts (Cuarentena de Datos)

```

{
    "id": "string (Auto-ID)",
    "targetDocumentId": "string (Cédula del ciudadano en conflicto)",
    "existingUserId": "string (UID del usuario que GANÓ)",
    "attemptedPayload": {
        "fullName": "string",
        "phone": "string",
        "address": "string",
        "recruitedBy": "string (UID del Multiplicador 'Perdedor')"
    },
    "conflictType": "string ('OFFLINE_RACE_CONDITION')",
    "status": "string ('PENDING REVIEW' | 'DISCARDED' | 'MERGED')",
    "timestamp": "timestamp",
    "resolvedBy": "string (UID Admin - Opcional)"
}

```

G. Colección voting_places (Lugares de Votación)

```
{  
    "id": "string (Código Único)",  
    "name": "string (Nombre del Puesto, ej: Col. San Francisco)",  
    "address": "string (Dirección física)",  
    "location": {  
        "type": "geopoint",  
        "geohash": "string",  
        "source": "string ('ADMIN_MANUAL' | 'GOOGLE_GEOCODED' | 'IMPORTED')"  
    },  
    "geoL1": "string",  
    "geoL2": "string",  
    "zone": "string (Zona, Comuna o Vereda)",  
    "tablesCount": "number (Cantidad total de mesas habilitadas)",  
    "potentialVoters": "number (Censo estimado del puesto - Opcional)",  
    "dayD_config": {  
        // [SCOPE FREEZE] IMPORTANTE:  
        // Estos campos existen en el esquema para evitar migraciones futuras,  
        // pero NO deben conectarse a ninguna vista del Dashboard en v1.0.  
        "witness_ids": [], // [SCOPE FREEZE] Placeholder estructural para FASE 3  
        // (v2.0). NO conectar a UI en v1.0.  
        "transport_coordinator_id": null, // [SCOPE FREEZE] Reservado para FASE 3  
        // (v2.0). Mantener null.  
        "e14_evidence": {  
            // Estructura reservada para mapa E-14  
            "Mesa_14": {  
                // "header_url": "gs://bucket/e14_p1_mesa14.webp",  
                // "body_url": "gs://bucket/e14_p2_mesa14.webp",  
                // "footer_url": "gs://bucket/e14_p3_mesa14.webp",  
                // "status": "VERIFIED"  
            }  
        }  
    },  
    "metadata": {  
        "updatedAt": "timestamp",  
        "verifiedBy": "string (UID Admin que validó la coordenada)",  
        "isActive": "boolean"  
    }  
}
```

H. Colección territorial_zones (Zonificación Dinámica)

```
{  
    "id": "string (Auto-ID, ej: 'zona_norte_01')",  
    "name": "string (Ej: 'Comuna 1 - Sector Bajo')",  
    "color": "string (Hex code para UI, ej: '#FF5733')",  
    "coordinatorId": "string (UID del responsable o ADMIN si está vacante)",  
    "zoneStatus": "string ('ACTIVE' | 'VACANT' | 'DISPUTED')", // 'DISPUTED' se  
    // activa automáticamente si hay Overlap > 1%  
    "version": "number (1)",  
    "geometry": {  
        "type": "Polygon",  
        "coordinates": [  
            [ [ ] ]  
        ]  
    }  
}
```

```

        [
            // IMPORTANTE: Orden GeoJSON es [Longitud (X), Latitud (Y)]
            [-75.281, 2.934], // Punto 1
            [-75.285, 2.935], // Punto 2
            [-75.283, 2.931], // Punto 3
            [-75.281, 2.934] // Cierre del polígono (Punto 1 == Último)
        ]
    ],
    "stats": {
        "assignedVoters": "number (Computed via Async Trigger)", // NO conteo en
        tiempo real
        "targetGoal": "number"
    },
    "metadata": {
        "createdAt": "timestamp",
        "updatedBy": "string"
    }
}

```

I. Colección message_templates (Builder Nativo)

```

{
    "id": "string (Auto-ID interno, independiente del SID)",
    "sid": "string (Twilio SID, null si está en borrador)",
    "friendlyName": "string (Ej: 'Invitación Evento Neiva')",
    "language": "string ('es')",
    "category": "string ('MARKETING' | 'UTILITY')",
    "status": "string ('DRAFT' | 'SUBMITTING' | 'APPROVED' | 'REJECTED')",
    "rejectionReason": "string (Visible solo si status == REJECTED)",
    "contentStructure": {
        "header": {
            "type": "string ('IMAGE' | 'TEXT' | 'NONE')",
            "mediaUrl": "string (URL temporal en GCS para vista previa)"
        },
        "body": "string (Texto con variables: 'Hola {{1}}...')",
        "footer": "string",
        "buttons": [
            { "type": "QUICK_REPLY", "text": "Confirmar Asistencia" }
        ]
    },
    "surveyConfig": {
        "enabled": "boolean",
        "questionText": "string (Enunciado principal)",
        "selectionMode": "string ('SINGLE' | 'MULTIPLE')",
        "constraints": {
            "minSelect": "number (Defecto: 1)",
            "maxSelect": "number (Defecto: 1 para SINGLE)"
        },
        "options": [
            { "id": "opt_1", "label": "Seguridad", "value": "SEC" },
            { "id": "opt_2", "label": "Salud", "value": "HLT" }
        ]
    },
}

```

```

"variablesMapping": ["firstName", "votingPlace"], // Sugerencia de mapeo
"metadata": {
    "createdBy": "string (UID Admin)",
    "createdAt": "timestamp",
    "lastTwilioSync": "timestamp"
}
}

```

J. Colección transfer_requests (Auditoría de Lealtad)

```

{
    "id": "string (Auto-ID)",
    "userId": "string (UID del Votante)",
    "currentLeaderId": "string (UID Líder Original)",
    "targetLeaderId": "string (UID Nuevo Líder - Dueño del QR escaneado)",

    "approverId": "string (UID del responsable: COORDINATOR o ADMIN según RF-1.12.C)",
    "reason": "string ('RELOCATION' | 'CONFLICT' | 'ERROR')",
    "status": "string ('PENDING' | 'APPROVED' | 'REJECTED')",
    "requestDate": "timestamp",
    "resolutionDate": "timestamp",
    "metadata": {
        "zoneId": "string" // Para filtrar en el dashboard correcto
    }
}

```

K. Colección events (Logística de Convocatoria)

```

{
    "id": "string (Auto-ID)",
    "title": "string (Ej: 'Reunión Líderes Comuna 1')",
    "description": "string",
    "startDateTime": "timestamp",
    "endDateTime": "timestamp",
    "location": {
        "address": "string",
        "geopoint": "geopoint (Lat/Lng del lugar)",
        "allowedRadius": "number (Metros, ej: 50)"
    },
    "status": "string ('ACTIVE' | 'CANCELLED' | 'COMPLETED')",
    "config": {
        "requireGeoCheckIn": "boolean (True = Exige estar en el sitio)",
        "pointsValue": null // [LEGACY] Campo inhabilitado en v1.0. Mantener en null.
    },
    "metadata": {
        "createdBy": "string (UID)",
        "createdAt": "timestamp"
    }
}

```

L. Colección event_attendance (Logs de Asistencia)

```
{
  "id": "string (Auto-ID)",
  "eventId": "string (Ref a collection 'events')",
  "userId": "string (Ref a collection 'users')",
  "timestamp": "timestamp (Hora del escaneo)",
  "checkInMethod": "string ('QR_SCAN' | 'MANUAL_OVERRIDE')",
  "validationData": {
    "userLocation": "geopoint (Donde estaba el usuario)",
    "distanceToEvent": "number (Metros calculados)",
    "isVerified": "boolean (True si distance < allowedRadius)"
  }
}
```

M. Colección political_campaigns (Instancia Electoral)

```
{
  "id": "string (Auto-ID)",
  "politicianId": "string (Ref a users where type='POLITICIAN')",
  "adminId": "string (Ref a users que administra)",
  "electionType": "string ('MAYORALTY' | 'GOVERNORSHIP' | 'PRESIDENCY' | 'COUNCIL' | 'ASSEMBLY' | 'CONGRESS')",
  "year": number,
  "scope": { // Para validación Geo-Fence
    "country": "string",
    "geoL1": "string | NULL",
    "geoL2": "string | NULL"
  },
  "branding": {
    "name": "string (Nombre corto para UI, ej: 'Alcaldía 2026')",
    "slogan": "string",
    "logoUrl": "string (URL pública en Storage - Formato PNG/SVG)",
    "primaryColor": "string (Hex Code, ej: '#003399')",
    "secondaryColor": "string (Hex Code, ej: '#FFCC00')",
    "ballotNumber": "string",
    "party": "string",
    "proposals": ["string"]
  },
  "status": "string ('ACTIVE' | 'ARCHIVED')",
  "settings": {
    "financials": {
      "minRechargeAmount": "number (10.00)",
      "maxHourlySpendLimit": "number (50.00)", // Circuit Breaker propio de esta
      campana
    },
    "alerts": {
      "minAlertAmount": "number (5.00)",
      "notificationRecipients": ["gerente@campanaA.com"] // Emails específicos
    },
    "financialAdmins": ["contador@campanaA.com"] // [ACL] Quién puede recargar
    AQUÍ
  },
  "election": {
    "electionDate": "timestamp", // Fecha crítica para RF-1.1
    "votingStationLockDays": "number (5)"
  }
}
```

```

        "allowLateFill": "boolean"
    },
    "goals": {
        "multiplierTarget": "number (10)", // Estrategia 1x10
        "linkTarget": "number (100)"
    },
    "communication": {
        "globalCommunityLink": "string (WhatsApp Channel)",
        "helpDeskPhone": "string"
    },
    "security": {
        "hqWhitelistedIps": ["201.234.xx.xx"] // IP de la Sede de ESTA campaña
(RF-8.7)
    },
    "hierarchy": {
        "COORDINATOR": {
            "enabled": boolean, // True por defecto. False para campañas planas.
            "label": "string", // Ej: "Gerente de Zona"
            // Restricción Crítica: Define el techo de la jerarquía
            "maxScopeLevel": "string ('geoL1' | 'geoL2' | 'geoL3')"
        },
        "LINK": {
            "enabled": boolean,
            "label": "string", // Ej: "Enlace"
            "maxScopeLevel": "string ('geoL3')"
        }
    }
}

```

N. Colección campaign_responses (Telemetría de Encuestas)

```
{
    "id": "string (Auto-ID)",
    "messagingCampaignId": "string (Ref a messaging_campaigns)",
    "userId": "string (Ref a users)",
    "type": "string ('BUTTON' | 'LIST')",
    "payload": "string (Valor técnico, ej: 'CONFIRM_ATTENDANCE')",
    "receivedAt": "timestamp"
}
```

O. Colección master_geo_structure (Configuración de Países)

```
{
    "id": "CO", // Document ID = Código de País
    "name": "Colombia",
    "phonePrefix": "+57",
    "hierarchy": {
        "11": { "label": "Departamento", "required": true },
        "12": { "label": "Municipio", "required": true },
        "13": { "label": "Comuna/Corregimiento", "required": false }
    },
    "validationRegex": {
        "phone": "^3[0-9]{9}$" // Regla específica por país
    }
}
```

```
    }  
}
```

P. Colección notifications (Bandeja de Entrada de Usuario)

```
{  
  "id": "string (Auto-ID)",  
  "recipientId": "string (Ref a users)",  
  "type": "string ('SYSTEM' | 'ALERT' | 'ACHIEVEMENT' | 'TASK')",  
  "title": "string",  
  "body": "string",  
  "deepLink": "string (Ej: '/dashboard/disputes/123')",  
  "isRead": "boolean (false)",  
  "createdAt": "timestamp",  
  "expiresAt": "timestamp (TTL: 30 días para limpieza automática)"  
}
```

RF-4.3: Protocolo de Exportación y Prevención de Fugas (DLP)

- **Restricción de Acceso (RBAC):** La exportación en formato plano (Excel/CSV) es una capacidad exclusiva del rol **ADMIN**. * *Nota Operativa:* Los Coordinadores y Enlaces **NO** tienen permisos de descarga de base de datos (Ver Matriz RF-8.2). Para labores de logística física o punteo, deben utilizar estrictamente la herramienta de "**Listados de Punteo (PDF)**" definida en el **RF-7.8**, la cual genera documentos trazables y optimizados para impresión.
- **Modos de Exportación (Admin):** Al ejecutar una exportación, el sistema dispone de dos esquemas de datos según la sensibilidad requerida:

A. MODO MASTER (Privilegiado):

- *Propósito:* Copias de seguridad (Backup), migraciones o auditoría interna.
- *Contenido:* Volcado total de la colección users. Incluye documentId completo, phone, address exacta (texto), geopoint (lat/long) y metadatos de sistema.

B. MODO OPERATIVO (Safe-Field / DLP):

- *Propósito:* Compartir métricas con consultores externos, prensa o equipos de estrategia que no requieren realizar contacto directo ni visitas.
- *Esquema de Columnas (Sanitizado):*

1. **Identidad Visual:** Nombre Completo (Visible). 2. **Identidad Legal (Enmascarada):** documentId se transforma a formato *****1234. Mantiene la unicidad para conteo sin revelar la cédula real.

2. **Ubicación (Nivel Barrio / Manzana):**

- **Datos Permitidos:** Se exportan las jerarquías territoriales estructurales: location.geoL1 (Departamento), location.geoL2 (Municipio) y **location.geoL3 (Barrio, Comuna o Vereda)**, así como la calculatedZoneId (Zona de Campaña).
- **Supresión Estricta (Sanitización):** Se eliminan del archivo los campos **location.address** (Nomenclatura exacta: Calle/Carrera/Número) y **location.geopoint** (Coordenadas Lat/Lng).
- **Justificación Operativa:** El "Barrio" es un dato público necesario para la logística de movilización (agrupación para transporte/buses), mientras que la "Dirección Exacta" es un dato privado sensible que no aporta valor a la estrategia macro y aumenta el riesgo de seguridad física del votante en caso de filtración.

3. **Contacto:** El campo phone se excluye o se enmascara (300***567) para evitar el robo de base de datos para telemarketing externo.

4. **Estructura:** Incluye Rol, Fecha de Registro y Nombre del Líder (recruitedBy).

• **Protocolo de Notificación Activa (Security Broadcast):**

- **Disparador:** El sistema detecta la solicitud de exportación bajo el esquema MODO MASTER.
- **Mecanismo:** Antes o durante la generación del archivo, se dispara una tarea asíncrona de notificación prioritaria.
- **Destinatarios (Principio de Transparencia):** Se envía una alerta vía Email (y WhatsApp si está configurado como canal crítico) a:

- **Todos los demás usuarios con rol ADMIN:** Para que el equipo de campaña se entere si uno de sus miembros está extrayendo datos.
- **El rol SUPER_ADMIN (Soporte Técnico):** Como auditor neutral externo a la operación política.

- **Contenido de la Alerta:** "ALERTA DE SEGURIDAD: Se ha iniciado una descarga de la Base de Datos Maestra (Datos Sensibles) realizada por el usuario [Nombre] desde la IP [IP Address]. Fecha: [Timestamp]."
- **Excepción:** La exportación en MODO OPERATIVO (Datos sanitizados para prensa/operación) no dispara esta alerta crítica, solo genera log pasivo.

- **Protocolo de Marcado Forense (File Fingerprinting):**

- **Objetivo:** Garantizar que cualquier archivo descargado contenga evidencia intrínseca de su origen y responsable, dificultando la negación plausible en caso de filtración.
- **Estructura del Archivo:** Independientemente del formato (CSV o Excel), el sistema inyectará obligatoriamente un **Encabezado de Auditoría** en las primeras filas, desplazando los datos reales hacia abajo:
 - Row 1: "CONFIDENCIAL - PROPIEDAD DE [NOMBRE CAMPAÑA]"
 - Row 2: "Responsable de Custodia: [Nombre Admin] (UID: [Admin_UID])"
 - Row 3: "Fecha de Generación: [Timestamp UTC] | Traza ID: [Audit_Log_ID]"
 - Row 4: (Vacío)
 - Row 5: [Cabeceras de Columnas: Cédula, Nombre, etc...]
- **Naming Convention:** El nombre del archivo descargado seguirá el patrón estricto: DATA_LEAK_TRACE_[Audit_Log_ID].csv.

- **Nota de Integridad:** El sistema almacena el Audit_Log_ID en la base de datos. Si aparece un archivo "huérfano" o renombrado, el Admin puede abrirlo, leer la Row 3 y cruzar ese ID con el sistema para identificar quién lo descargó originalmente.

RF-4.4: Definición de Índices Compuestos (Performance)

Para garantizar tiempos de respuesta < 1s en los Dashboards (RNF-1) y soportar las consultas del RF-7.2 (Data Scoping), se deben desplegar los siguientes índices compuestos en la colección users:

A. Índices de Rendimiento (Leaderboards y Métricas):

Estos índices permiten ordenar usuarios por desempeño dentro de un territorio específico sin descargar toda la base de datos.

Nombre del Índice (Query Scope)	Campos (Orden)	Justificación (Uso en Dashboard)
Ranking Municipal	location.geoL2 (Asc) + metrics.recruitedCount (Desc)	Permite mostrar "Los mejores líderes de Neiva" (RF-7.1).
Crecimiento Reciente	location.geoL2 (Asc) + metadata.createdAt (Desc)	Gráficos de "Nuevos usuarios hoy" filtrados por ciudad (RF-7.1).
Ranking por Zona	location.calculatedZoneId (Asc) + metrics.recruitedCount (Desc)	Ranking de líderes dentro de un polígono/barrio específico.
Distribución de Roles	location.geoL2 (Asc) + role (Asc)	Gráficos de Dona (Multiplicadores vs. Seguidores) (RF-7.1).
Búsqueda en Rama	hierarchyPath (Array) + searchKey (Asc)	Permite al Multiplicador buscar por nombre filtrando estrictamente dentro de su red descendente (RF-7.6).

Nombre del Índice (Query Scope)	Campos (Orden)	Justificación (Uso en Dashboard)
Búsqueda en Zona	location.calculatedZoneId (Asc) + searchKey (Asc)	Permite al Coordinador buscar por nombre filtrando estrictamente dentro de su territorio (RF-7.6).

B. Índices de Operación y Campañas:

Estos índices optimizan la segmentación para mensajería y logística.

Nombre del Índice	Campos (Orden)	Justificación
Audiencia WhatsApp	whatsappConsent (Asc) + location.city (Asc)	Filtrado rápido para campañas masivas segmentadas (RF-5.1).
Logística Día D	votingStationId (Asc) + role (Asc)	Listar testigos o líderes asignados a un puesto de votación específico. Estado: [INACTIVO v1.0] . Se puede desplegar, pero no se usará en consultas de esta versión.
Jerarquía Directa	parentId (Asc) + metadata.createdAt (Desc)	Permite a un multiplicador ver su propia red ordenada por fecha de ingreso (RF-7.2).

C. Consideraciones de Despliegue:

- Archivo de Configuración:** Estos índices deben residir en `firestore.indexes.json` para ser desplegados automáticamente mediante `firebase deploy --only firestore:indexes`.
- Exenciones de Indexación (Cost Optimization & Write Protection):** Para reducir los costos de almacenamiento (RNF-7) y prevenir errores de límites de índice ("Index Entry Limit Exceeded") en documentos con mapas anidados complejos, se debe configurar el archivo `firestore.indexes.json` para

excluir explícitamente los siguientes campos de la indexación automática (Single Field Index Exemptions):

Colección	Campo Exento	Justificación Técnica
audit_logs	details	Contiene el mapa changes (before/after) ¹ . Indexar el historial de cambios de cada perfil triplica el costo de escritura. Las búsquedas se hacen por actorId o timestamp, no por el contenido del cambio.
message_templates	contentStructure	Objeto JSON que define el diseño visual (Header/Body/Footer) ²²² . No se requiere realizar consultas filtrando por la estructura interna del diseño.
users	consent_evidence	Datos de auditoría legal (IP, UserAgent) ³³³ . Estos datos se consultan accediendo directamente al documento del usuario por su ID, nunca mediante búsquedas globales (Collection Group Queries).
users	metadata	Específicamente el subcampo sourceQr si solo se busca por coincidencia exacta, o metadatos técnicos que no requieran ordenamiento.

D. Consideración de Integridad (Write Cost): Para garantizar el cumplimiento del RF-1.9 sin lecturas recursivas costosas (que agotarían la cuota de Firestore), la validación se basa estrictamente en la inspección del array hierarchyPath del nodo destino, lo cual es una operación en memoria de costo O(1) y no requiere lecturas adicionales a la base de datos.

E. Especificación de Despliegue (firestore.indexes.json): Para evitar errores de despliegue y garantizar el funcionamiento de los filtros combinados (Zona + Rol + Tiempo), se debe incluir el siguiente bloque en la configuración del proyecto.

Índice Crítico de Operación (Filtrado Avanzado): Este índice permite responder a

la pregunta: "¿Cuáles son los nuevos Multiplicadores en la Zona Norte ordenados por fecha de ingreso?".

```
{  
  "indexes": [  
    {  
      "collectionGroup": "users",  
      "queryScope": "COLLECTION",  
      "fields": [  
        { "fieldPath": "location.calculatedZoneId", "order": "ASCENDING" },  
        { "fieldPath": "role", "order": "ASCENDING" },  
        { "fieldPath": "metadata.createdAt", "order": "DESCENDING" }  
      ]  
    },  
    {  
      "collectionGroup": "users",  
      "queryScope": "COLLECTION",  
      "fields": [  
        { "fieldPath": "location.city", "order": "ASCENDING" },  
        { "fieldPath": "role", "order": "ASCENDING" },  
        { "fieldPath": "metrics.recruitedCount", "order": "DESCENDING" }  
      ]  
    },  
    {  
      "collectionGroup": "users",  
      "queryScope": "COLLECTION",  
      "fields": [  
        { "fieldPath": "hierarchyPath", "arrayConfig": "CONTAINS" },  
        { "fieldPath": "searchKey", "order": "ASCENDING" }  
      ]  
    },  
    {  
      "collectionGroup": "users",  
      "queryScope": "COLLECTION",  
      "fields": [  
        { "fieldPath": "location.calculatedZoneId", "order": "ASCENDING" },  
        { "fieldPath": "searchKey", "order": "ASCENDING" }  
      ]  
    }  
  ],  
  "fieldOverrides": []  
}
```

- **Nota de Optimización (Index Scope):** Se define explícitamente queryScope: "COLLECTION" para todos los índices de la colección users. Esto restringe la indexación exclusivamente a la colección raíz, reduciendo el costo de escritura y almacenamiento en un 50% comparado con un índice recursivo (COLLECTION_GROUP) que no es necesario dada la arquitectura plana del RF-4.1.

RF-4.5: Arquitectura de Agregación Asíncrona (Event-Driven Metrics) Para garantizar el rendimiento del registro (RNF-1) y la integridad en escenarios Offline (RNF-3), los contadores y métricas NO se calculan en el cliente.

- **Mecanismo de Disparo (Trigger):**

- Se despliega una *Cloud Function* vinculada al evento `onWrite` de la colección `users`.

- **Lógica de Agregación (Idempotente):**

1. **Evento `onCreate`:** Si se crea un usuario nuevo, el sistema identifica su `recruitedBy` (Líder) y su `calculatedZoneId` (Territorio).

- **Acción Estándar:** Incrementa atómicamente (`FieldValue.increment(1)`) el contador `recruitedCount` del Líder y el `assignedVoters` de la Zona.

- **Nota Técnica de Escalabilidad (Fragmentación de Contadores / Sharded Counters):** Para evitar errores de contención (write-hotspots) en nodos de alto tráfico (ej: Totales Globales de Campaña o perfil del Candidato) donde se supere 1 escritura/segundo:

- **Escritura:** La Cloud Function distribuye el incremento en un fragmento aleatorio de una subcolección shards.

- **Lectura:** El cliente agrega (suma) los valores de los fragmentos para mostrar el total.

2. **Evento `onUpdate` (Cambio de Líder):** Si un usuario es reasignado de Líder A a Líder B.

- Acción: Decrementa (-1) al Líder A y Incrementa (+1) al Líder B en una transacción atómica.

3. **Evento `onDelete`:** Si un usuario es eliminado.

- Acción: Decrementa (-1) los contadores asociados.
- **Latencia Esperada:** La actualización de los contadores en el Dashboard tendrá una "Consistencia Eventual" (retraso estimado de 500ms - 2s), lo cual es aceptable para reportes operativos.

RF-4.6: Reglas de Seguridad y Protección de Esquema (Firestore Rules)

- **Mandato de Congelamiento (Scope Freeze Enforcement):**
 - **Objetivo:** Garantizar la integridad evolutiva del sistema asegurando que los campos marcados en el esquema como [SCOPE FREEZE] (Reservados para Fase 3, ver RF-4.2.G) sean técnicamente inmutables durante la versión actual (v1.0).
 - **Implementación Técnica:** Se deben desplegar *Firebase Security Rules* que prohíban explícitamente la escritura o modificación de estos campos, **incluso para usuarios con rol ADMIN**.
 - **Lógica de Regla:**
 - Para la colección voting_places, campo dayD_config:
allow write: if request.resource.data.dayD_config ==
resource.data.dayD_config; (El dato nuevo debe ser idéntico al viejo, es decir, sin cambios).
 - *Fallback:* Si el documento es nuevo, el campo debe ser null o venir vacío según la definición del esquema.
 - **Justificación:** Esto actúa como un "Cortafuegos de Datos". Evita que datos logísticos corruptos, parciales o no validados (como asignación de testigos o transporte) contaminen la base de datos operativa antes de que el Módulo del Día D esté auditado y liberado oficialmente.

4.5 MÓDULO 5: INTEGRACIÓN CON WHATSAPP (TWILIO)

RF-5.1: Motor de Mensajería y Bloqueo por Consentimiento (Hard Opt-in)

El sistema utiliza Twilio Programmable Messaging bajo una política de cero tolerancias al spam:

- **Filtro de Audiencia (Query Level):** Al crear una campaña, la consulta a la base de datos incluye explícitamente la cláusula `where whatsappConsent == true`. Los usuarios con `false` o `null` son invisibles para el motor de envíos.
- **Activación de importados y Protocolo de Calentamiento (Warm-up Strategy):**
 - **Validación de Presupuesto:** El sistema verifica el saldo disponible contra el volumen total y solicita confirmación de 'Gasto Excepcional' si supera el límite horario.
 - **Restricción de Salud de Línea (Health Score Guard):** Para evitar bloqueos por parte de Meta al contactar usuarios "fríos" (Cold Start), se aplica una regla específica para el segmento `origin == 'CSV_IMPORT'`:
 - **Límite de Volumen:** Se establece un tope máximo técnico de **500 mensajes / día** para este origen.
 - **Agendamiento en Cascada (Batching):** Si el Administrador intenta enviar una campaña a 2,000 usuarios importados, el sistema **NO bloquea** el envío, sino que lo fragmenta automáticamente:
 - *Día 1:* Envía los primeros 500.
 - *Día 2, 3 y 4:* Programa tareas diferidas (Cloud Tasks scheduled) para el resto, notificando al Admin: "*Por seguridad de la línea, esta campaña se entregará progresivamente durante 4 días.*"
- **Bloqueo de Seguridad (Pre-Send):**
 - Incluso si se intenta forzar el envío a un ID específico, el servicio de mensajería verifica: `if (!user.metrics.whatsappConsent) return ERROR_CONSENT_REQUIRED`.
 - Esto previene errores humanos o intentos de enviar mensajes a usuarios que revocaron el permiso después de la segmentación inicial.
- **Validación de Integridad de Plantilla (HSM Check):**
 - **Requisito Previo:** Antes de permitir que una campaña pase de DRAFT a SCHEDULED, el backend ejecuta una consulta a la API de Twilio (Content API) para verificar el estado actual del templateSid.
 - **Regla de Bloqueo:**
 - SI `status == 'APPROVED'`: Se permite el agendamiento y se guarda `templateReviewStatus: 'APPROVED'`.
 - SI `status != 'APPROVED'`: Se lanza un error bloqueante: "La plantilla seleccionada no ha sido aprobada por Meta o está en revisión. No se puede programar el envío."

- **Reporte de Exclusión:** En las estadísticas de la campaña, estos usuarios se clasifican como "**Omitidos por Privacidad**" (no suman al costo ni a la tasa de error).

- **Adaptador de Salida (Output Adapter):** El servicio de mensajería debe implementar un patrón de adaptador que seleccione el proveedor según el entorno:

- ```
const smsProvider = process.env.NODE_ENV ===
 'production'
 ? new TwilioLiveProvider() // Gasta dinero real
 : new TwilioMockProvider(); // Simula latencia y
 respuestas, costo $0
```

- **Arquitectura de Envío Asíncrono (Background Task Delegation):**

- **Problema:** El envío iterativo de campañas a audiencias masivas (ej: > 500 usuarios) dentro del ciclo de vida de una petición HTTP o Cloud Function estándar provoca errores de *Timeout* (Gateway Time-out 504) y estados de campaña inconsistentes.
- **Solución:** Se implementa el patrón Productor-Consumidor utilizando **Google Cloud Tasks**.

- **Productor (Campaign Dispatcher):** Al aprobar la campaña, el sistema no envía los mensajes directamente. En su lugar, itera la audiencia y **encola** una tarea individual por cada destinatario en la cola campaign-delivery-queue.
- **Consumidor (Worker):** Una Cloud Function aislada procesa cada tarea, realiza la petición a la API de Twilio y registra el estado inicial.
- **Control de Velocidad (Rate Limiting):** La cola se configura con un maxDispatchesPerSecond ajustado al límite de la API de WhatsApp (ej: 80 MPS) para evitar errores 429 y proteger la calidad de la línea telefónica.

**RF-5.2: Gestión de Invitaciones (No Invasivo)** El sistema envía automáticamente un Enlace de Invitación Único tras el registro, en lugar de agregar usuarios a grupos forzosamente.

#### A. Mecanismo de Disparo (Trigger):

- Se ejecuta de forma asíncrona (Cloud Function) inmediatamente después de que el sistema confirma la persistencia del usuario (onCreate en colección users).

- **Categoría:** El mensaje se clasifica como UTILITY para aprovechar la tarifa reducida definida en system\_config.financials.costPerMessageUtility.

## B. Protocolo de "Fallo Seguro" Financiero (Fail-Safe Policy) [NUEVO]:

- **Contexto:** Dado que el registro de votantes es la operación crítica (RF-1.1), la falta de fondos **NUNCA** debe impedir la creación del usuario en la base de datos.
- **Lógica de Verificación (Pre-Send Check):**

1. Antes de invocar la API de Twilio, el sistema consulta el saldo disponible en la colección wallet\_transactions (snapshot calculado).

2. **Regla de Bloqueo:** IF (walletBalance < costPerMessageUtility):

- **Acción 1 (Omisión):** Se aborta el envío del SMS. No se realiza ninguna llamada a la API de Twilio (evitando errores 402 o deuda técnica).
- **Acción 2 (Integridad):** El registro del usuario (users) permanece **ACTIVO** y exitoso.
- **Acción 3 (Auditoría):** Se genera un registro en audit\_logs con actionType: 'SKIPPED\_NOTIFICATION' y details: {'reason': 'INSUFFICIENT\_FUNDS', 'targetId': uid}.

- **Justificación:** Esto cumple con la restricción de "Bloqueo si Costo > Saldo" del **RF-5.6** sin violar el principio de disponibilidad y captura de datos del **RNF-3**.

## C. Feedback de Usuario (Política de Silencio / Silent Fallback):

- **Escenario:** Si el sistema omite el envío del SMS debido a la activación del protocolo "Fallo Seguro" (Saldo Insuficiente), la PWA debe comportarse ante el usuario exactamente igual a un escenario de éxito total.
- **Acción UI:**

0. Se muestra el mensaje estándar de éxito: "Registro Guardado Exitosamente".

1. Se despliega el Modal de Bienvenida con el video del candidato (ver RF-3.7), garantizando la gratificación inmediata.

- **Prohibición:** Queda estrictamente PROHIBIDO mostrar alertas, *toasts* o mensajes de error al usuario final indicando que el SMS no se envió (ej: "*No pudimos enviar la notificación*").
- **Justificación:** La falta de saldo es una incidencia administrativa del ADMIN, no un error operativo del usuario. Revelar este estado causa desconfianza en la solvencia de la campaña.

### RF-5.3: Constructor Nativo de Plantillas (WhatsApp Template Builder)

**Objetivo:** Permitir a los administradores crear, visualizar y gestionar el ciclo de vida de las plantillas HSM (Highly Structured Message) sin salir de la aplicación.

- **A. Editor Visual de Plantillas:**

- **Interfaz:** Formulario estructurado que replica las capacidades de la API de Twilio Content.

- **Componentes Soportados:**

- **Cabecera (Header):** Texto (Negrita), Imagen, Video o Documento.
- **Cuerpo (Body):** Área de texto con soporte para variables.
  - **Monitor de Costo en Tiempo Real:** Debajo del área de texto, se debe renderizar un widget de cotización:

- **Visualización:** "Caracteres: 155/160 | Segmentos SMS: 1 | Multiplicador de Costo: x1".
- **Alerta de Codificación:** Si el usuario inserta un emoji o carácter especial, el indicador cambia a "Modo Unicode (UCS-2)" y recalcula el límite a 70 caracteres por segmento.
- **Warning:** Si segmentCount > 1, el contador se torna naranja para advertir sobre el sobrecosto en canales SMS.

- **Pie de Página (Footer):** Texto gris pequeño.

- **Botones (Actions):** Soporte para *Call to Action* (Ir a Web, Llamar) y *Quick Reply* (Sí/No).

- **B. Motor de Envío a Aprobación (Submission Engine):**

- **Acción:** Al guardar, el sistema envía una petición POST a la API de Twilio Content.
- **Manejo de Estado:** La plantilla queda en estado local SUBMITTED\_TO\_META hasta recibir el webhook de resolución.

- **C. Gestión de Rechazos:**

- Si Meta rechaza la plantilla, el sistema captura la razón del rechazo (ej: "Formato promocional agresivo") y permite al usuario editar el borrador para reintentar.

- **D. Configuración de Encuestas (Survey Logic):**

- **Objetivo:** Permitir al administrador estructurar preguntas para la recolección de datos estructurados (Data Enrichment) directamente desde el canal de mensajería.
- **Definición del Cuestionario:** El constructor debe permitir definir:
  - **Enunciado:** Texto de la pregunta (puede ser parte del *Body* o un bloque separado).
  - **Opciones de Respuesta:** Lista definida de valores posibles (ej: "Sí", "No", "Tal Vez" o "Educación", "Salud", "Seguridad").
  - **Modalidad de Selección:**
    - **Única (Single Select):** El votante solo puede elegir una opción (Radio Button behavior).
    - **Múltiple (Multi Select):** El votante puede marcar varias opciones (Checkbox behavior).

- **Restricciones de Cantidad (Cardinalidad):**

- Si es *Múltiple*, el creador debe poder estipular la cantidad **Mínima** (ej: "Elige al menos 1") y **Máxima** (ej: "Elige máximo 3 prioridades") de respuestas permitidas.

- **Renderizado Técnico:** El sistema seleccionará automáticamente el componente de UI más adecuado en WhatsApp (Botones de Respuesta Rápida, Lista Interactiva o WhatsApp Flows) según la complejidad y longitud de las opciones configuradas.

#### RF-5.6: Calculadora y Billetera Virtual (Prepago Dinámico)

- **Fuente de Costos (Lista de Precios Interna / SSOT):** El sistema utiliza **estrictamente** los valores almacenados en la colección system\_config (financials.costPerMessage) como la única autoridad para el cálculo de presupuestos.
  - **Prohibición de Consultas Externas:** Para garantizar la velocidad de la interfaz (RNF-1) y la predictibilidad del gasto, se **prohíbe** consultar la API de Precios de Twilio durante el diseño o envío de la campaña.
  - **Naturaleza del Costo (Precio Operativo):** Este valor representa el precio final pactado con la campaña. Incluye un margen de seguridad sobre la tarifa técnica del proveedor destinado a:
    - Cubrir fluctuaciones cambiarias.
    - Sostener la infraestructura del sistema.
    - **Absorber costos técnicos ocultos** (como tarifas de señalización de mensajes fallidos) para permitir una política de "**Reembolso Total al Usuario**" sin generar deuda técnica en la billetera visible.
    - **Abstracción Transaccional (Meta Policy Wrapper):** Aunque Meta factura por "Sesión de 24hs", el sistema expone internamente un modelo de **Costo por Envío Único**.
      - *Justificación:* Dado que el protocolo **RF-5.8** bloquea las respuestas de los usuarios (No-Chat), no existe la posibilidad operativa de mantener una sesión abierta o "gratuita" mediante interacciones continuas. Por tanto, cada notificación enviada por el Admin equivale técnicamente al inicio de una nueva conversación facturable.
  - **Actualización:** La modificación de este valor es un proceso administrativo manual. Cualquier cambio solo afecta a campañas futuras, respetando el "Snapshot de Costo" de las ya creadas.
- **Pre-Flight Check (Calculadora de Segmentos y Protocolo Híbrido):**
  - **Detección de Canal:** El sistema verifica el messageType o canal de entrega.
    - **Caso WhatsApp (Modelo de Conversación):**

- **Lógica de Asignación:** Se ignora el conteo de caracteres y se asigna segmentCount = 1.
- **Selección de Tarifa (Dynamic Pricing):** El sistema determina el costo base consultando la configuración global (system\_config) según el tipo de mensaje definido en la campaña:
  - IF messageType == '**UTILITY**' (ej: OTPs, Confirmaciones) → Aplica financials.costPerMessageUtility.
  - ELSE (Defecto/Marketing) → Aplica financials.costPerMessage.
- **Cálculo Final:** appliedCost = Tarifa\_Seleccionada \* Audiencia.
- **Caso SMS:** Se ejecuta el algoritmo de segmentación técnica:
  - *Encoding Check:* Detecta si hay caracteres especiales (tildes, emojis, ñ) que fuercen codificación **UCS-2** (Límite 70 caracteres). Si es texto estándar, usa **GSM-7** (Límite 160 caracteres).
  - *Cálculo:* segmentCount = Math.ceil(bodyLength / limit).
- **Proyección de Gasto:** Presupuesto Total = Audiencia \* (system\_config.costPerMessage \* segmentCount).
- **Snapshot de Costo (appliedCost):**
  - Al aprobar la campaña, se guarda en la base de datos el valor calculado: messaging\_campaigns.config.appliedCost = Costo\_Base \* segmentCount.
  - *Integridad:* Este valor se convierte en la "Tarifa Congelada" para auditoría y reembolsos, protegiendo a la campaña de fluctuaciones o errores de cálculo posteriores.
- **Protocolo de Integridad Transaccional (ACID Compliance):**
  - **Problema:** En escenarios de alta concurrencia (ej: 50 workers de Cloud Tasks procesando una campaña masiva simultáneamente), lecturas paralelas del saldo pueden provocar "Doble Gasto" (Double Spending), permitiendo consumos superiores al saldo real disponible.
  - **Mandato Técnico:** Toda operación que implique la **deducción de saldo** (Gasto) o la **modificación de crédito** (Recarga) debe ejecutarse obligatoriamente dentro de una **Transacción Atómica de Base de Datos** (Firestore Transaction).
  - **Lógica de Ejecución (Read-Modify-Write):**

- **Lectura Bloqueante:** La transacción lee el documento actual de la billetera.
  - **Validación en Memoria:** Calcula Saldo\_Nuevo = Saldo\_Actual - Costo. Si Saldo\_Nuevo < 0, lanza una excepción y aborta la transacción (Rollback).
  - **Escritura Atómica:** Si la validación pasa, escribe el nuevo saldo y el registro del log (wallet\_transactions) en el mismo instante.
- **Resolución de Conflictos:** Si el saldo cambia externamente mientras la transacción se ejecuta (Contención), el driver de la base de datos debe **reintentar** automáticamente la operación con el nuevo valor actualizado, garantizando consistencia matemática exacta.
  - **Modelo de Recarga: Protocolo de Segregación de Funciones (SoD) y Estrictamente Manual (Centralizado).**
    - **Decisión de Arquitectura:** Se descarta la integración de pasarelas de terceros (Stripe/Wompi) en la v1.0 para garantizar el control centralizado del presupuesto y facilitar la auditoría legal de los recursos de campaña.
    - **Mecanismo:** El saldo se inyecta mediante una transacción administrativa directa en la base de datos (Dashboard Admin).
    - **Restricción de Autoridad (Financial Allowlist):** Para ejecutar una recarga, el usuario debe cumplir **simultáneamente** dos condiciones:
      - Tener el rol ADMIN en su perfil (para acceder al Dashboard).
      - Tener su email listado explícitamente en system\_config.security.financialAdmins.
    - **Objetivo:** Evitar que personal técnico (DevOps, Soporte IT) con acceso administrativo pueda alterar el presupuesto sin responsabilidad legal.
    - **Alerta de Seguridad:** Cualquier modificación manual a la lista financialAdmins en la base de datos dispara una notificación crítica inmediata a todos los correos actualmente en esa lista.
  - **SLA de Acreditación de Saldo (Service Level Agreement):**
    - **Tiempo de Respuesta:** < 2 Horas hábiles desde la solicitud formal del Coordinador al Admin.
    - **Protocolo de Emergencia (Día D):** < 15 Minutos. Se requiere disponibilidad de un "Oficial de Presupuesto" con acceso root al Dashboard durante la jornada electoral.

- **Auditoría y Unicidad (Idempotency Check):** Toda recarga (DEPOSIT) debe incluir obligatoriamente en el campo metadata.reference el número de comprobante bancario o acta física.
  - **Regla de Bloqueo (Anti-Duplicidad):** Antes de procesar el ingreso de saldo, el sistema ejecuta una consulta de verificación en la colección wallet\_transactions.
    - **Condición:** Si ya existe un documento activo con type == 'DEPOSIT' Y metadata.reference == [Valor Ingresado].
    - **Acción:** El sistema **rechaza la transacción** y muestra el error: "*Duplicidad Detectada: El comprobante [Referencia] ya fue procesado el [Fecha]*".
    - **Objetivo:** Garantizar una relación 1:1 estricta entre los movimientos bancarios reales y el saldo virtual, previniendo la inflación accidental del presupuesto por parte del **ADMIN**.
- **Bloqueo:** Si Costo > Saldo, se deshabilita el envío de la campaña.
- **Protocolo de Parada de Emergencia (Financial Circuit Breaker):**
  - **Objetivo:** Detener hemorragias financieras causadas por bucles infinitos (errores de código) o errores humanos (campañas duplicadas masivas).
  - **Configuración:** Se define una variable campaign.settings.financials.maxHourlySpendLimit (Ej: \$50.00 USD) en la configuración global.
  - **Lógica de Evaluación:** Antes de cada envío (pre-send hook), el sistema consulta:
    - SUM(amount) en wallet\_transactions donde type == 'SPEND' y timestamp > (NOW - 1 HOUR).
  - **Acción de Disparo:** Si el acumulado supera el límite maxHourlySpendLimit:
    - **Pausado de Infraestructura (Queue Freeze):** El sistema invoca la API de Cloud Tasks para **PAUSAR** la cola campaign-delivery-queue. Esto detiene el consumo de presupuesto inmediatamente, dejando los mensajes pendientes en estado "Encolado" hasta que un Admin audite y reanude.
    - **Congelamiento:** El estado de la campaña en curso cambia forzosamente a PAUSED\_SAFETY.
    - **Notificación Crítica:** Se envía un correo urgente al Admin: "*ALERTA DE SEGURIDAD: Se ha bloqueado el sistema por consumo inusual (\$51.00 en 10 min). Revise logs.*"

- **Desbloqueo:** Solo un usuario con rol ADMIN puede reactivar el servicio pulsando un botón de [RESET SAFETY LOCK] tras auditar el error.
- **Monitor de Salud Financiera (Low Balance Alert):** Se implementa un disparador ("Trigger") post-transacción que evalúa la solvencia de la billetera:
  - **Disparador:** Se ejecuta cada vez que se crea un documento de tipo SPEND en la colección wallet\_transactions.
  - **Lógica del Umbral (Dynamic Threshold):**
    - El sistema recupera el burnRate (Gasto Promedio Diario de los últimos 7 días, ver RF-7.1).
    - **Regla:** SI ( $walletBalance < (\text{burnRate} * 0.10)$ ) O ( $walletBalance < \text{system\_config.minAlertAmount}$ ).
    - *Interpretación:* Se alerta si el saldo no cubre el 10% del consumo diario habitual o si cae por debajo de un monto fijo de seguridad (ej: \$5.00 USD).
- **Acción:**
  - Envío de Email prioritario a los usuarios con rol ADMIN.
  - **Envío de Alerta WhatsApp (Categoría UTILITY):** Se dispara automáticamente una plantilla de alta prioridad (ej: system\_alert\_low\_balance) al teléfono verificado del Administrador Principal.
    - *Justificación:* Garantiza la entrega inmediata en la pantalla de bloqueo del responsable financiero, utilizando la tarifa más baja del proveedor (costPerMessageUtility) y evitando las colas de mensajes masivos de marketing.
    - Registro de la alerta en audit\_logs para constancia de aviso.
  - **Frecuencia (Anti-Spam):** La alerta se silencia por 24 horas después de dispararse para evitar saturación, a menos que el saldo llegue a 0.
- **Política de Moneda y Visualización (Currency & Precision Standards):**
  - **Moneda Base (Single Source):** Para garantizar la integridad contable y evitar discrepancias por fluctuación cambiaria (TRM), el sistema opera, almacena y visualiza saldos estrictamente en **Dólares Estadounidenses (USD)**.
    - *Restricción de UI:* Queda prohibida la implementación de conversores automáticos a Pesos Colombianos (COP) en los componentes de saldo, para evitar la percepción de "pérdida de dinero" pasiva por devaluación diaria.

- **Estándar de Precisión (Rounding Logic):**

- **Backend (Ledger):** Los cálculos de costo y almacenamiento en base de datos (wallet\_transactions) se manejan con **4 decimales** de precisión (ej: \$0.0452) para absorber micro-costos de mensajería sin errores de redondeo acumulativo.
- **Frontend (Visualización):** La interfaz debe truncar visualmente a **2 decimales** estándar (ej: \$0.04), utilizando un sufijo de moneda explícito.
- **Formato de Salida:** "\$ " + value.toFixed(2) + " USD". (Ejemplo visual: **\$ 50.00 USD**).

#### RF-5.7: Protocolo de Garantía de Entrega y Reembolsos (Webhook Handler)

El sistema implementa un modelo de facturación justo ("Fair Billing") basado en el éxito técnico de la entrega, procesado de forma asíncrona.

- **A. Captura de Estado (Webhook):**

- Se expone un endpoint POST /api/webhooks/twilio-status que recibe los eventos de cambio de estado de cada mensaje individual (MessageSid).
- **Mapeo de Estados:**

- **Éxito (Cargo Final):** sent, delivered, read.
- **Fallo (Reembolsable):** failed (Error técnico/autenticación), undelivered (Número inexistente/bloqueado).

- **Protocolo de Coherencia Eventual (State Monotonicity Logic):**

- **Problema:** Debido a la concurrencia de red, es posible recibir el evento DELIVERED antes que el evento SENT. Procesarlos en orden de llegada causaría que el mensaje retroceda falsamente a un estado anterior.
- **Solución:** Se implementa una **Matriz de Peso de Estado** para validar las transiciones. El sistema solo actualiza el registro en la base de datos si el peso del nuevo estado es **mayor** al actual.

- **Peso 1:** queued, accepted (Inicialización).

- **Peso 2:** sent (En red).
- **Peso 3:** delivered (Entregado al dispositivo).
- **Peso 4 (Terminal):** read, failed, undelivered.

- **Regla de Descarte:** IF (NewState.Weight <= CurrentState.Weight) THEN Ignorar Webhook.

- *Ejemplo:* Si el mensaje ya está marcado como delivered (Peso 3) y llega un webhook tardío de sent (Peso 2), el sistema responde 200 OK pero **no toca la base de datos**.

- **B. Lógica de Reembolso Automático:**

- **Condición de Disparo:** Al recibir un evento de fallo (failed o undelivered), el sistema verifica dos condiciones atómicamente:

- El messagingCampaignId asociado existe.
- **Check de Transición:** El estado anterior en la base de datos **NO** era ya un estado de fallo.

- **Justificación:** Esto garantiza la **Idempotencia Financiera**. Si el webhook de fallo llega duplicado, la segunda vez será ignorada por la lógica de pesos ( $4 \leq 4$ ) o por este chequeo, evitando devolver dinero dos veces por el mismo mensaje.
- **Acción Financiera:** Se crea una transacción de abono en wallet\_transactions cumpliendo la **Regla de Simetría**:

- type: 'REFUND'.
- amount: **Debe ser idéntico** al valor registrado en messaging\_campaigns.config.appliedCost (el costo congelado al momento del envío).
- **Manejo de Discrepancias (Billing Absorption):**

- *Escenario:* Si Twilio cobra una tarifa parcial por el intento fallido (ej: "Carrier Handover Fee"), esta diferencia **NO se traslada al usuario.**
- *Resolución:* El sistema (bajo el rol SUPER\_ADMIN) absorbe cualquier costo técnico residual contra el margen de seguridad operativo. El saldo del usuario (ADMIN) se restaura como si la transacción nunca hubiera ocurrido.
- *Auditoría:* No se requiere acción manual. La discrepancia queda implícita en la diferencia entre el saldo de la cuenta bancaria de Twilio y el saldo virtual total del sistema.

- **Balance:** El saldo de la billetera se incrementa inmediatamente.

- **C. Protocolo de Revocación por Bloqueo (Hard Opt-out Logic):**

- **Justificación:** Cumplimiento estricto del RF-5.1 y prevención de degradación del "Health Score" de la línea.
- **Disparador:** Si el webhook reporta estado failed o undelivered Y el payload contiene el Error Code 21610 ("Attempt to send to unsubscribed recipient").
- **Acción de Base de Datos:** El sistema ejecuta una actualización atómica sobre el documento del usuario en la colección users:

- 1. Revocación:** Establece el campo metrics.whatsappConsent a false. Esto excluye automáticamente al usuario de futuras consultas de audiencia (RF-5.1).
- 2. Auditoría:** Genera un registro en audit\_logs con actionPerformed: 'SYSTEM\_REVOKE\_OPT\_OUT' para dejar constancia de que no fue una acción manual.

- **Nota de Flujo:** Esta acción ocurre en paralelo al reembolso (Punto B). El fallo genera devolución de dinero por el intento fallido, y la revocación evita intentos futuros.

- **D. Actualización de Métricas:**

- El contador messaging\_campaigns.stats.failed se incrementa.
- El costo total messaging\_campaigns.stats.totalCost se ajusta a la baja para reflejar el gasto real auditado.

- **E. Webhook de Estado de Plantillas:**

- **Endpoint:** POST /api/webhooks/twilio-template-status.
- **Lógica:** Cuando Meta aprueba o rechaza una plantilla, Twilio envía un evento. El sistema actualiza el campo status de la plantilla y, si es REJECTED, guarda el motivo.

#### **RF-5.8: Protocolo de Interacción Híbrida (Hybrid Interaction Logic)**

El sistema evoluciona de un bloqueo total a un filtro selectivo que permite la recolección de datos estructurados sin habilitar canales de conversación abierta.

#### **A. Webhook de Clasificación de Tráfico (Traffic Filter & Sorter):**

- **Endpoint:** POST /api/webhooks/twilio-inbound
- **Lógica de Discriminación:** Al recibir un mensaje entrante, el sistema evalúa su naturaleza:

0. **Señal de Datos (Payloads):** Si el mensaje es una respuesta interactiva (ButtonResponse o ListResponse).

- **Acción:** El sistema **PROCESA** el payload (lo guarda en campaign\_responses), actualiza métricas y **DETIENE** cualquier respuesta automática.
- **Impacto Financiero:** Esta acción tiene **Costo \$0** para el usuario, ya que ocurre dentro de la sesión de 24h pagada con el envío de la plantilla original.
- **Acción de Agregación:** Al recibir un payload válido, el sistema ejecuta una transacción atómica sobre el documento messaging\_campaigns relacionado:
  - Incrementa stats.replied en +1.

- Incrementa la clave específica en stats.responseDistribution (ej: stats.responseDistribution.CONFIRM\_YES +1).
- *Justificación RNF-7:* Esto pre-calcula los datos para el Dashboard, permitiendo cargar las estadísticas de la campaña con **una sola lectura** (Cost-Saving), en lugar de contar documentos uno por uno.

1. **Ruido (Conversacional):** Si el mensaje es Texto Libre (Body) o Multimedia (NumMedia > 0).

▪ **Política de Cero Almacenamiento (Zero-Storage Policy):**

- *Recepción Pasiva:* El sistema recibe el webhook de Twilio identificando la presencia de adjuntos (NumMedia > 0) y sus URLs temporales (MediaUrl).
- *Bloqueo de Ingesta:* El backend **ignora explícitamente** estas URLs. Queda estrictamente **PROHIBIDO** descargar el archivo binario o re-subirlo a Google Cloud Storage (GCS).
- *Justificación:* Evitar la facturación por almacenamiento de "basura digital" (memes, cadenas, audios) y anular riesgos legales asociados a la posesión de contenido sensible no solicitado.

- **Acción de Respuesta:** El sistema dispara la Auto-Respuesta de Desvío (RF-5.8.B) informando que el canal no procesa estos archivos.
- **Frecuencia:** La auto-respuesta se limita a 1 vez cada 24h para proteger el saldo (Anti-Loop).

## B. Plantilla de Desvío (Disclaimer):

- **Contenido:** "🤖 *Sistema Automático:* Esta línea no recibe mensajes, audios ni llamadas. 🤷 Para atención humana, contacta a tu Líder ({{LeaderName}}) aquí: ⏬ <https://wa.me/{{LeaderPhone}}> O únete al canal oficial: {{GlobalLink}}"

**C. Control de Frecuencia (Anti-Loop):** Para proteger el presupuesto (RF-5.6), la auto-respuesta solo se dispara una vez cada 24 horas por usuario, independientemente de cuántos mensajes o fotos envíe en ese periodo.

#### D. Validación de Encuesta (Survey Processor):

- Al recibir una interacción (Webhook), el sistema consulta el surveyConfig de la campaña activa.

- **Check de Cardinalidad:**

- Si mode == 'MULTIPLE', el sistema acumula las respuestas entrantes en una ventana de tiempo (Sesión de Encuesta) o valida si el payload entrante (en caso de usar *Flows*) cumple con minSelect <= respuestas <= maxSelect.

- **Persistencia:** Las respuestas validadas se almacenan en la colección campaign\_responses como un array en el campo payload (ej: ['SEC', 'HLT']).

### RF-5.9: Mecanismo de Reconciliación de Saldos (The Financial Sweeper)

Proceso de auditoría automatizada para garantizar la consistencia entre el saldo descontado en DB y el gasto real en Twilio, cubriendo escenarios de pérdida de webhooks.

#### A. Arquitectura del Proceso:

- **Tipo:** Cron Job (Cloud Scheduler).
- **Frecuencia:** Cada 4 horas.
- **Objetivo:** Detectar y corregir transacciones "zombies".

#### B. Lógica de Detección (Query):

El sistema busca en la colección de logs de mensajes aquellos que cumplan:

1. **Estado Transitorio:** status IN ['queued', 'sending', 'sent'] (Aún no tienen confirmación final de entrega o fallo).
2. **Antigüedad:** createdAt < (NOW - 2 HOURS). (Se asume que si en 2 horas no ha llegado webhook, se perdió).

**C. Acción de Recuperación (Polling Selectivo):** Para cada mensaje "zombie" detectado:

1. **Consulta API:** Se ejecuta client.messages(sid).fetch() contra Twilio para obtener el estado real.
2. **Sincronización:** Se actualiza el estado local en DB.
3. **Disparo de Reembolso:** \* Si la API responde que el mensaje terminó en undelivered o failed, el script invoca programáticamente la función de **Reembolso Automático** definida en el RF-5.7.
  - *Resultado:* El dinero regresa a la billetera del candidato automáticamente, aunque el webhook original haya fallado.

#### **RF-5.10: Matriz Centralizada de Notificaciones (Notification Router)**

**Objetivo:** Orquestar el envío de alertas del sistema seleccionando el canal más eficiente según la criticidad del evento y el costo asociado.

##### **A. Definición de Canales:**

- **PUSH (Web Push):** Canal prioritario y gratuito para usuarios con la PWA instalada. Requiere permiso del navegador.
- **IN-APP (Bandeja):** Persistencia en base de datos (ícono de campana). Visible al abrir la aplicación.
- **EMAIL (Transaccional):** Para auditoría, seguridad y reportes extensos.
- **SMS/WA (Mensajería):** Canal de costo. Reservado exclusivamente para OTPs y Alertas Financieras Críticas (Server Down / Wallet Empty).

##### **B. Matriz de Eventos por Rol:**

| Evento<br>(Disparador)                 | Destinatario<br>(Rol) | Canal<br>Primario         | Canal<br>Secundario<br>(Fallback) | Justificación                             |
|----------------------------------------|-----------------------|---------------------------|-----------------------------------|-------------------------------------------|
| <b>Código OTP<br/>(Login/Registro)</b> | Todos                 | <b>WhatsApp /<br/>SMS</b> |                                   | Crítico para<br>acceso. Costo<br>asumido. |

|                                        |                       |                 |            |                                                       |
|----------------------------------------|-----------------------|-----------------|------------|-------------------------------------------------------|
| <b>Nuevo Seguidor Registrado</b>       | Multiplicador / Líder | <b>PUSH</b>     | IN-APP     | Gratificación inmediata (Gamificación) sin costo.     |
| <b>Meta Alcanzada (Zona/Personal)</b>  | Líder/Coord           | <b>PUSH</b>     | IN-APP     | Refuerzo positivo.                                    |
| <b>Alerta de Fraude (Velocidad)</b>    | Coordinador           | <b>EMAIL</b>    | IN-APP     | Requiere auditoría y traza formal.                    |
| <b>Saldo Bajo (&lt; 10%)</b>           | Admin (Financiero)    | <b>EMAIL</b>    | <b>SMS</b> | Riesgo de parada operativa. Amerita costo de SMS.     |
| <b>Solicitud de Traslado (Disputa)</b> | Coordinador           | <b>IN-APP</b>   |            | Tarea administrativa no urgente (se ve en Dashboard). |
| <b>Exportación de Datos (DLP)</b>      | Super_Admin / Admin   | <b>EMAIL</b>    |            | Alerta de Seguridad (RF-4.3).                         |
| <b>Recordatorio "Votar Mañana"</b>     | Seguidor              | <b>WhatsApp</b> |            | Campaña masiva (Costo Marketing).                     |

#### **C. Regla de Silencio (Do Not Disturb):**

- Las notificaciones **PUSH** de tipo "Motivacional" (Nuevo Seguidor, Meta) se silencian automáticamente entre las 22:00 y las 06:00 (Hora Local), acumulándose solo en la bandeja **IN-APP**. Las alertas de Seguridad/Infraestructura ignoran esta regla.

## **4.6 MÓDULO 6: GEOLOCALIZACIÓN Y MAPAS**

### **RF-6.1: Estrategia Híbrida y Normalización**

**1. GPS (Hardware):** Prioridad 1. Costo: \$0.

**2. Online (Interactivo):** Uso de **Google Places Autocomplete API**.

- **Eficiencia:** El usuario selecciona una dirección sugerida que ya contiene las coordenadas (lat/long).
- **Impacto:** No requiere geocodificación en el servidor.
- **Alcance:** Exclusivo para la **Ubicación de Vivienda** (RF-1.1 / Campo Dirección).
- **Excepción:** La ubicación del **Puesto de Votación** NO utiliza esta API en el cliente; se rige por las coordenadas estáticas pre-cargadas en la colección voting\_places (ver RF-1.1 actualizado).
- **Protocolo de Fallo (Fallback Strategy):**
  0. **Escenario:** Si la API de Google retorna error (Quota Exceeded, Billing Error) o no carga por lentitud de red (> 3s).
    1. **Acción UI:** El componente de Autocomplete se desmonta automáticamente y es reemplazado por un campo de texto estándar (<input type="text" />).
    2. **Restricción Técnica:** Se PROHÍBE explícitamente el uso de APIs públicas gratuitas (como Nominatim/OSM) en el cliente para evitar bloqueos por violación de Términos de Servicio (ToS) en producción.
    3. **Procesamiento:** El dato ingresado manualmente se trata idéntico a un "Registro Offline" (ver Punto 3), enviándose a la cola de geocodificación diferida en el servidor.

**3. Offline (Diferido):** Input de texto plano.

- **Procesamiento:** **Google Maps Geocoding API** (Server-Side via Cloud Functions).
- **Disparador:** Se ejecuta únicamente durante la sincronización de registros que tienen location.type == 'MANUAL\_TEXT' y coordenadas vacías.

**RF-6.4: Visualización Híbrida (Cost-Saving)** Producción: Google Maps Platform. Desarrollo/Fallback: OpenStreetMap (Leaflet) para reducir costos.

**RF-6.5: Control de Presupuesto de Geocodificación y UX de Degradación (Circuit Breaker)** Mecanismo para evitar facturación excesiva por geocodificación masiva de datos offline.

- **Lógica de "Solo Necesario":** El sistema verifica si el registro entrante ya tiene coordenadas (provenientes del GPS del móvil o del Autocomplete online). Si existen, se omite la llamada a la API de Geocoding.
- **Cuotas Diarias:** Se configura en system\_config un límite diario de solicitudes (Ej: 500 peticiones/día = \$2.50 USD).
- **Fallback de Agotamiento:** Si se supera el límite diario:

1. El sistema detiene el proceso de geocodificación automática.
2. Los registros quedan marcados con estado geoStatus: 'PENDING\_RETRY'.
3. **Protocolo de "Deuda Geográfica" (Store & Forward):**

- **No Bloqueo:** El sistema **permite guardar el registro exitosamente** sin coordenadas. El usuario ve el aviso "Guardado (Sin Mapa)".
- **Estado de Estacionamiento:** El registro queda marcado en base de datos con geoStatus: 'PENDING\_RETRY' y un contador retryCount: 0.
- **Política de Reintento (Next-Day Priority):** Estos registros acumulados tienen **prioridad de ejecución** sobre los nuevos registros del día siguiente. El sistema intentará geocodificarlos automáticamente en el lote de las 02:00 AM (ver RF-6.7) hasta agotar el nuevo presupuesto diario disponible.

- **Alertas:** Notificación al Admin si el consumo alcanza el 80% del presupuesto diario asignado a mapas.
- **UX de Degradación Elegante (Fallback UI):** El componente de Mapa en el Frontend debe estar envuelto en un límite de error (Error Boundary).

## Disparadores:

1. Fallo de carga del script de Google Maps (Error de Red).
2. Retorno de error de API (Quota Exceeded / BillingDisabled).
3. Detección de "Modo Ahorro" activado globalmente por el Admin.

## Comportamiento Visual (Component Swap):

- **Eliminación de "Espacios Muertos":** El sistema NO muestra un cuadro gris, ni un icono de imagen rota, ni un mapa en blanco. El componente de mapa se desmonta completamente del DOM (unmount).
- **Tarjeta de Reemplazo (Placeholder Activo):** El espacio liberado es ocupado inmediatamente por el componente <OfflineLocationWidget />.
- **Transición Transparente:** El sistema detecta el fallo del proveedor de mapas y conmuta el input.

1. Antes: "Buscar dirección en Google..." (Con icono de lupa/mapa).
2. Despues (Fallback): "Escribe la dirección exacta manualmente" (Con icono de lápiz/texto).

- **Feedback al Usuario:** Se muestra un pequeño indicador textual (caption): "*Servicio de mapas no disponible. Tu dirección será validada posteriormente por el sistema.*"

## • Elementos Visuales:

1. **Icono de Estado:** Una ilustración vectorial simple (SVG) de un "Satélite Tachado" o "Nube Offline" en colores neutros (Gris/Naranja tenue).
2. **Micro-Copy:** Un mensaje directo: "*Sin acceso a mapas. Actuando en Modo Manual.*"
3. **Expansión de Formulario:** Los campos de texto (Departamento, Municipio, Dirección), que normalmente están

ocultos o minimizados, se expanden automáticamente con el foco (autofocus) puesto en el primer campo seleccionable.

### Integridad de Datos:

4. El campo location.type cambia automáticamente de 'GPS' a 'MANUAL\_TEXT'. \* El sistema permite guardar el registro sin coordenadas, encolándolo para geocodificación diferida (ver RF-6.1 Punto 3).

## RF-6.6: Gestión Territorial por Polígonos (Geofencing Político)

### A. Definición de Zonas (Dashboard Admin):

- **Herramienta de Dibujo:** Implementación de DrawingManager (Google Maps JavaScript API) en el Dashboard. Permite a los coordinadores dibujar, editar y eliminar polígonos irregulares sobre el mapa para definir sus territorios.
- **Restricción de Topología (Solid Polygons Only / No Donuts):**
  - **Regla:** El sistema soporta estrictamente **Polígonos Simples**. No se admite la creación de zonas con "agujeros" o islas internas (Donuts).
  - **Validación Técnica:** El array de coordenadas GeoJSON debe contener **un único anillo lineal** (el borde exterior). Si el dibujo contiene anillos internos, el sistema rechazará el guardado.
  - **Solución Operativa:** Si un territorio rodea completamente a una zona excluida (ej: un parque o una base militar), el Coordinador debe dibujar la zona en forma de "C" (Herradura) o dividirla en dos sectores (Norte/Sur) que rodeen el obstáculo, garantizando que el polígono sea siempre sólido y continuo.
- **Optimización de Geometría (Performance Guardrail):**
  - **Problema:** El cálculo de pertenencia (Point-in-Polygon) en móviles puede bloquear la interfaz si la geometría es excesivamente compleja.
  - **Límite de Vértices:** Se establece un máximo técnico de **100 vértices** por zona.

- **Auto-Simplificación (Sanitización):** Al terminar de dibujar (evento overlaycomplete), el cliente verifica la cantidad de coordenadas.
  - **Acción:** Si vertices > 100, se ejecuta automáticamente turf.simplify(polygon, {tolerance: 0.0001, highQuality: false}).
  - **Resultado:** Reduce la carga computacional en un 90% manteniendo la forma visual del territorio casi idéntica, garantizando fluidez en dispositivos de gama baja.
- **Protocolo de Integridad de Edición (Optimistic Concurrency Control):**
  - **Objetivo:** Evitar que dos usuarios con permisos sobre la misma área (ej: un Coordinador y el Admin Central) sobrescriban el trabajo del otro si editan simultáneamente.
  - **Mecanismo (Version Check):**
    - **Lectura:** Al cargar el polígono en el editor, el sistema almacena localmente el número de versión actual (ej: v5).
    - **Escritura:** Al guardar, la transacción en Firestore incluye una pre-condición: solo actualizar SI version\_en\_base\_de\_datos == 5.
    - **Resolución:**
      - Si coincide: Se guardan los cambios y el servidor incrementa atómicamente versión a 6.
      - Si falla (Collision): El sistema rechaza el guardado y alerta al usuario.
  - **Feedback UI:** Se muestra un mensaje bloqueante (Toast Error): "*Conflictivo de Edición: Alguien más ha modificado este territorio mientras trabajabas. El mapa se recargará para mostrar los nuevos límites.*" (Esto fuerza al usuario a ver los cambios ajenos antes de reaplicar los suyos).
- **Protocolo de Auditoría Forense de Límites (Anti-Gerrymandering Snapshot):**

- **Objetivo:** Permitir la trazabilidad visual y la reversión de cambios en las fronteras territoriales, previniendo que un Coordinador altere maliciosamente sus límites para excluir zonas de bajo rendimiento o apropiarse de zonas ajenas.
- **Captura de Evidencia (Snapshotting):**

- Cada vez que se guarda una modificación en una zona, el sistema genera obligatoriamente un registro en la colección audit\_logs.
- **Payload Crítico:** El campo details.changes.before debe almacenar el objeto GeoJSON completo (geometry.coordinates) tal como existía **antes** de la edición.

- **Visualización Forense:**

- En el "Historial de Cambios" del Dashboard (disponible para el Admin), al seleccionar un evento de edición de mapa, el sistema debe ser capaz de renderizar **ambas capas** (la "Fantasma/Anterior" en gris punteado y la "Nueva" en color sólido) para facilitar la inspección visual del cambio realizado.

- **Validación Topológica (Soft-Overlap Policy & Multi-Guard):**

- **1. Pre-Validación de Complejidad (Hard Stop):**

- **Detección:** Antes de procesar cualquier lógica de negocio, el sistema calcula en el cliente (Turf.js) con cuántos polígonos activos intersecta el nuevo dibujo.
- **Regla de Bloqueo:** Si el nuevo polígono intersecta con **más de 1 zona existente** simultáneamente.
- **Acción:** Se impide el guardado y se muestra una alerta de error (Toast Rojo): "*Error de Topología: El territorio invade múltiples zonas vecinas ([Lista]). Por favor ajusta los bordes para resolver los conflictos de uno en uno.*"

- **Justificación:** La interfaz de resolución de disputas (RF-6.6.C) requiere estrictamente conflictos binarios (1 vs 1) para funcionar matemáticamente.

- **2. Detección de Conflicto Simple (Warning):**

- **Condición:** Si existe intersección con **exactamente 1 zona** y el área superpuesta es **> 1%**.
- **Interacción (Modal):** Se interrumpe el guardado silencioso y se muestra un Modal de Decisión:

- *Título:* "Conflicto Territorial Detectado"
- *Mensaje:* "El territorio dibujado se superpone con la **[Nombre Zona Existente]**. ¿Deseas mantener ambas zonas?"
- *Opciones:* [CANCELAR/CORREGIR] o [GUARDAR COMO DISPUTA].

- **3. Resolución del Estado (Persistencia):**

- Si el Admin confirma la opción [GUARDAR COMO DISPUTA]:
  - La **nueva zona** se crea con zoneStatus: 'DISPUTED'.
  - La **zona antigua** afectada actualiza automáticamente su estado a zoneStatus: 'DISPUTED'.

- **4. Visualización de Conflicto (UI Feedback):**

- **Estilo Obligatorio (Visibilidad Diferenciada):**

- **Roles Estratégicos (ADMIN / COORDINATOR):** Visualizan la alerta crítica. Los polígonos DISPUTED se renderizan con **Patrón de Rayas Diagonales** y bordes rojos para forzar la resolución.

- **Roles Tácticos (LINK / MULTIPLIER):** Aplica el principio de "**Abstracción Operativa**".

- *Visualización:* El usuario de campo ve la zona como sólida y normal (ACTIVE). **NO** ve rayas ni mensajes de error.
- *Acción de Registro:* El sistema permite el guardado del votante sin advertencias bloqueantes.
- *Atribución Provisional:* En el backend, si la coordenada cae en la intersección de dos zonas disputadas, el sistema asigna el votante automáticamente a la **Zona más antigua** (por createdAt) para permitir el cálculo inmediato de metas, sujeto a re-cálculo silencioso una vez el Admin resuelva el conflicto.
- **Objetivo:** Que el conflicto sea evidente visualmente en el mapa estratégico, forzando a los coordinadores a renegociar los límites físicos mediante el Panel de Resolución.

- **5. UI de Resolución de Disputas (Protocolo de Saneamiento):**

- **Disparador:** Al hacer clic sobre una zona marcada con patrón de rayas (DISPUTED), el Dashboard no muestra la info estándar, sino el **Panel de Resolución**.
- **Interfaz:** Muestra el nombre de las dos zonas en conflicto (ej: "Zona A" vs. "Zona B") y el área superpuesta en metros cuadrados.
- **Acciones de Resolución Rápida (Boolean Ops):**

- **Botón [ CEDER A VECINO ]:**

- **Lógica:** La zona seleccionada pierde el área de superposición.

- **Técnica:** Turf.difference(Zona\_Actual, Zona\_Vecina).

▪ **Botón [ RECLAMAR TODO ]:**

- **Lógica:** La zona seleccionada se expande y "come" el área superpuesta de la vecina.
- **Técnica:** Turf.difference(Zona\_Vecina, Zona\_Actual) (Recorta a la otra).

▪ **Botón [ EDITAR VÉRTICES ]:**

- **Habilita los manejadores (handles) para corrección manual punto a punto.**
- **Resultado:** Tras la operación, si la intersección baja del 1%, ambas zonas pasan automáticamente a estado ACTIVE y desaparece el patrón de rayas.

• **Protocolo de Intervención Administrativa (Deadlock Breaker):**

Si una zona permanece en estado DISPUTED por más de 48 horas sin resolución entre los Coordinadores involucrados:

- **Notificación:** El sistema alerta al **ADMIN**.
- **Resolución Forzada (God Mode):** El Admin adquiere permisos de escritura sobre ambos polígonos para redibujar los límites y cerrar la disputa unilateralmente desde su Dashboard Global.

• **Estandarización de Datos (GeoJSON Adapter):** \* **Backend (Storage):** Los polígonos se almacenan estrictamente en formato **GeoJSON** ([Lng, Lat]) para permitir el procesamiento directo con **Turf.js** en las Cloud Functions.

- **Frontend (Render):** Dado que la API de Google Maps requiere objetos literales {lat, lng}, el cliente debe implementar un **Adaptador Bidireccional**:

- *Al leer (DB -> Mapa):* Convierte el array GeoJSON a google.maps.LatLngLiteral.

- *Al guardar (Mapa -> DB)*: Convierte el dibujo del usuario al array GeoJSON antes de enviarlo al servidor.

- **Visualización de Acefalía (Vacantes):**

- El componente de mapa debe renderizar los polígonos con zoneStatus: 'VACANT' con un estilo visual distintivo (ej: Relleno Gris con patrón de rayas o borde punteado rojo).
- **Interacción:** Al hacer clic en una zona vacante, el Dashboard del Admin debe mostrar un botón de acción rápida: **[ASIGNAR NUEVO COORDINADOR]**, que abre un modal para buscar y vincular un usuario existente a ese territorio.

- **Restricción de Edición por Resolución (Viewport & Precision Guard):**

- **Criterio de Habilitación:** Las herramientas de dibujo y edición de vértices (DrawingManager) se activan dinámicamente basándose en el ancho de pantalla disponible (`window.innerWidth >= 768px`), **independientemente de si el dispositivo es táctil o tiene mouse**.
- **Soporte para Tablets:** Se autoriza explícitamente la edición de mapas en iPads y Tablets Android. Se recomienda el uso en **Modo Horizontal (Landscape)** para mayor precisión.
- **Bloqueo en Teléfonos (Small Screens):** En dispositivos con ancho < 768px, el mapa entra forzosamente en modo "Solo Lectura" para evitar la corrupción de polígonos por falta de precisión táctil ("Fat-Finger Error").
- **Feedback Inteligente (Responsive Alert):**

- *Caso Tablet Vertical:* Si el dispositivo es capaz pero está en orientación incorrecta, muestra: "Para editar zonas, por favor **gira tu dispositivo a posición horizontal.**"
- *Caso Teléfono:* Si la pantalla es físicamente pequeña, muestra: "Edición deshabilitada en teléfonos. Usa una Tablet o PC."

## **B. Motor de Asignación Automática (Point-in-Polygon):**

- **Disparador:** Al momento del registro (RF-1.1), cuando el sistema captura la latitud/longitud (`location.type == 'geopoint'`).

- **Lógica de Cálculo:**

1. **Cliente (Online):** Utiliza `google.maps.geometry.poly.containsLocation(point, polygon)` para asignar la zona en tiempo real y mostrarla en la UI.
  2. **Servidor (Offline/Validación):** Si el registro llega por sincronización diferida, una Cloud Function utiliza la librería **Turf.js** para procesar geométricamente la coordenada contra la colección territorial\_zones y asignar el zoneld correcto.
- **Fallback:** Si la coordenada queda fuera de todos los polígonos dibujados, se asigna a una zona por defecto llamada "Zona Sin Asignar" para revisión manual.

**C. Protocolo de Excepción (Zona Limbo / Catch-All)** Define el tratamiento de las coordenadas que caen en "Tierra de Nadie" (espacios vacíos entre polígonos o nuevas urbanizaciones no mapeadas).

1. **Asignación de Sistema:** Si el algoritmo *Point-in-Polygon* retorna false para todas las zonas activas, el campo calculatedZoneld se asigna automáticamente al valor reservado: **ZONE\_UNCATEGORIZED**.
2. **Implicación Estadística (Dual Reporting):**

- **Métricas Globales (Macro):** El usuario **SUMA** en los totales de la Ciudad y el Departamento (para no afectar el censo real del candidato).
- **Métricas de Rendimiento (Micro):** El usuario **NO SUMA** en la meta de ningún líder territorial específico, evitando distorsiones en los KPIs de cumplimiento de zona.

3. **Mecanismo de Corrección y Asignación de Responsabilidad:**

- **Enrutamiento de la Alerta (Hierarchy Fallback):** Dado que la ubicación no pertenece a ninguna zona activa, el sistema dirige la alerta al **Coordinador Jerárquico** (el superior directo en la rama del Multiplicador que capturó el dato, identificado vía `hierarchyPath`).
  - **Visualización:** En el Dashboard de este Coordinador, aparece el widget: "Hay [N] usuarios de tu red fuera de zona".

#### ○ Acciones Resolutivas (SoD):

- **A. Expandir Territorio:** Si el punto está adyacente a la zona actual del Coordinador (error de frontera), este puede editar su polígono para incluirlo (Conforme permisos de RF-6.6.A).
- **B. Asignación Manual (Parche):** Si el punto es lejano o aislado, el Coordinador debe forzar el manualZoneld a su zona para no perder la métrica, o notificar al **ADMIN** si se trata de un nuevo barrio que requiere crear una zona nueva.

**D. Protocolo de Reclutamiento Cruzado (Cross-Zone Logic)** Define el tratamiento de registros donde la calculatedZoneld del Votante difiere de la assignedZoneld de su Líder inmediato.

1. **Validación de Admisión:** El registro se acepta exitosamente (HTTP 200). No se bloquea la operación.

#### 2. Impacto en Métricas (Doble Contabilidad):

- **Ranking Personal (Leaderboard):** El registro SUMA al contador recruitedCount del Líder y cuenta para **tu histórico de rendimiento y estatus de liderazgo**.
- **Meta Territorial (KPI de Zona):** El registro NO SUMA a la meta de cumplimiento territorial de la zona del Líder.

- *Ejemplo:* Si el Líder A (Meta: Zona Norte) recluta a alguien del Sur, su avance en "Meta Zona Norte" se mantiene igual, pero la "Saturación Zona Sur" aumenta.

#### 3. Visibilidad para Coordinadores:

- El Coordinador de la Zona del Votante (Zona Sur) verá aparecer un "Voto Foráneo" en su mapa, marcado con una referencia al líder original: "*Votante gestionado por Líder de Zona Norte*". Esto asegura que el territorio se cubra sin duplicar esfuerzos de visita.

#### 4. Feedback Visual al Líder (Geo-fencing Warning):

- **Condición:** Se activa si calculatedZoneld != leader.assignedZoneld.
- **Visualización:** Toast/Banner de color Ámbar/Naranja (advertencia, no error).

- **Mensaje Estándar:** "¡Registro Exitoso! Nota: El votante vive en [Nombre Zona Detectada], fuera de tu territorio. Este registro suma a tu Red Personal, pero NO cuenta para tu Meta de Zona."
- **Justificación UX:** Evita reclamos falsos sobre fallos en las barras de progreso de cumplimiento de metas (RF-7.1).

## E. Trigger de Re-Zonificación (Topology Update Listener) [NUEVO]:

- **Contexto:** Cuando un Coordinador edita los vértices de un polígono existente (RF-6.6.A), la relación espacial de los usuarios asignados a esa zona puede cambiar, invalidando el estado actual de isCrossZone.
- **Mecanismo de Disparo:**

- **Trigger:** Evento onUpdate en la colección territorial\_zones.
- **Condición:** Se activa solo si el campo geometry ha cambiado (change.before.geometry != change.after.geometry).

- **Procesamiento Asíncrono (Cloud Task):**

- Debido a que una zona puede contener miles de usuarios, el cálculo no se realiza en tiempo real. El sistema encola una tarea de fondo: recalculate\_zone\_topology.
- **Query de Alcance:** El sistema selecciona todos los usuarios donde location.calculatedZoneId == ZoneID (Usuarios actuales de la zona).

- **Lógica de Actualización:** Para cada usuario recuperado:

1. **Re-validación Geométrica:** Ejecuta el algoritmo *Point-in-Polygon* (Turf.js) contra la *nueva* geometría de la zona.

- *Si sigue dentro:* No cambia el calculatedZoneId.
- *Si quedó fuera:* Cambia calculatedZoneId a ZONE\_UNCATEGORIZED (o busca en zonas vecinas si hay intersección).

2. **Recálculo de Flag:** Se re-evalúa la condición isCrossZone:

- IF (user.calculatedZoneId != user.leader.assignedZoneId) SET isCrossZone = true.

- **Impacto en UI:** El Coordinador verá actualizados los contadores de "Votos Foráneos" y las alertas de cruce de zona (RF-6.6.D) en los minutos posteriores a la edición del mapa.

## RF-6.7: Normalización Asíncrona (Arquitectura Productor-Consumidor)

Implementación de una cola de tareas (Cloud Tasks) para gestionar la geocodificación masiva de forma resiliente y controlada, evitando *Timeouts* en el servidor.

### A. Componente Productor (The Dispatcher):

- **Trigger:** Cloud Scheduler ejecuta el trabajo diariamente a las 02:00 AM.
- **Verificación Financiera:** Consulta `system_config.financials.dailyGeocodingBudget`. Si el presupuesto se agotó ayer, se restablece para el nuevo día.
- **Consulta Priorizada (FIFO):**
  - Busca documentos con `geoStatus == 'PENDING_RETRY'` (Deuda del día anterior). Orden ascendente por fecha (los más viejos primero).
  - Si sobra presupuesto, busca `geoStatus == 'PENDING'` (Nuevos registros offline/importados).
- **Regla de Agotamiento (Starvation Prevention):** Si un registro ha fallado por presupuesto o error técnico más de 3 veces (`retryCount > 3`), el sistema deja de intentarlo automáticamente y cambia su estado a `geoStatus: 'MANUAL REVIEW'` para que un humano lo ubique en el mapa manualmente, evitando costos infinitos en direcciones erróneas.
- **Encolado:** Por cada documento encontrado, crea una Tarea HTTP en la cola `geocoding-queue` con el payload: `{ userId: "...", address: "...", city: "..." }`.
- **Alcance:** Esto incluye tanto los registros manuales hechos en la PWA (Modo Offline) **como los registros masivos cargados vía Importador CSV (RF-1.11).**

### B. Configuración de la Cola (The Queue - Cloud Tasks):

- **Rate Limiting:** `maxDispatchesPerSecond: 5`.

- *Justificación:* Mantiene el consumo de la API de Google Maps fluido y evita picos que disparen alertas de seguridad o errores de cuota.
- **Retry Config:** maxAttempts: 3. Estrategia de *Exponential Backoff* para fallos de red.

### C. Componente Consumidor (The Worker):

- **Función:** Cloud Function individual activada por la cola.
- **Acción:**
  1. Recibe el payload de **un solo usuario**.
  2. **Validación Heurística (Pre-API Check):** Si la dirección tiene menos de 5 caracteres o coincide con patrones de basura conocidos (ej: "n/a", "no se", "mismo"), el sistema omite la llamada a Google, marca geoStatus: 'UNPROCESSABLE' y termina la ejecución (Costo \$0).
  3. **Ejecución:** Si pasa el filtro, llama a la Geocoding API de Google.
  4. **Clasificación de Resultado (Smart Cost-Control):**
    - **Caso A (Éxito):** Si la API devuelve coordenadas, actualiza location.geohash y ejecuta el *Point-in-Polygon*. Estado final: 'COMPLETED'.
    - **Caso B (Datos Inválidos):** Si la API retorna ZERO\_RESULTS (Google no encontró el lugar), se asume que la dirección está mal escrita.
      - **Acción:** Se marca **geoStatus: 'UNPROCESSABLE'**.
      - **Efecto:** Este estado es **TERMINAL**. El "Dispatcher" (Productor) ignorará este registro en las ejecuciones futuras, evitando gastar presupuesto en una dirección que ya sabemos que no existe.
    - **Caso C (Error Técnico):** Si hay *Timeout* o error 5xx, se incrementa el retryCount y se deja en 'PENDING\_RETRY' para que el Productor lo intente mañana.

## D. Protocolo de Resolución de Conflictos Geográficos (The Fixer UI):

- **Objetivo:** Proveer una interfaz de saneamiento para los registros que agotaron sus intentos de geocodificación automática (retryCount > 3) y quedaron en estado MANUAL REVIEW.
- **Responsable:** Coordinador de Zona (Perfil Estratégico - Desktop/Tablet).
- **Interfaz de Usuario (Dashboard):**

- **Ubicación:** Widget de "Alertas de Integridad" o módulo de Mapas.
- **Visualización:** Lista de tareas pendientes filtrada por el alcance geográfico del usuario (RF-7.2).

- **Flujo de Corrección:**

1. **Selección:** El Coordinador abre un registro fallido. El sistema muestra la dirección de texto original que falló (ej: "Frente a la tienda de Doña Marta").
2. **Pin Manual:** Se despliega el mapa interactivo (Google Maps) centrado en la ciudad/municipio del votante. El Coordinador debe ubicar visualmente el predio y soltar un PIN (Drag & Drop).
3. **Confirmación y Recálculo:**

- Al guardar, el sistema actualiza location.geopoint con la coordenada manual.
- Cambia el estado geoStatus a 'COMPLETED'.
- **Disparador Crítico:** Invoca inmediatamente la lógica **Point-in-Polygon** del RF-6.6 para determinar el nuevo calculatedZonel basado en la corrección.

- **Impacto en Métricas:**

1. El registro deja de ser un "dato flotante" y pasa a sumar inmediatamente en la meta de saturación de la zona identificada (territorial\_zones.stats.assignedVoters).
- **Auditoría:** Se genera un registro en audit\_logs con actionPerformed: 'MANUAL\_GEO\_FIX', documentando quién realizó la corrección.

## 4.7 MÓDULO 7: DASHBOARDS Y MÉTRICAS

**RF-7.1: Dashboard Principal y Definición de KPIs:** El sistema debe renderizar los siguientes indicadores, calculados dinámicamente según el Alcance Geográfico (Scope) del usuario (RF-7.2).

- **Contexto de Campaña y UX Multi-Entidad (Campaign Switcher):**
  - **Ubicación:** Cabecera (Header) de la aplicación, junto al logo o nombre de la campaña actual.
  - **Indicador Visual:** Se muestra el logo/avatar de la campaña activa actual. Si el usuario pertenece a más de una campaña (`memberships.length > 1`), aparece un indicador de despliegue (flecha/chevron).
  - **Interacción (Cambio Rápido):** Al pulsar el indicador, se despliega una lista ("Bottom Sheet" en móvil, "Dropdown" en escritorio) con las campañas vinculadas. Al seleccionar una, el Dashboard se recarga completamente filtrando todos los datos por el nuevo campaignId.
  - **Persistencia:** El sistema recuerda la última campaña seleccionada (`lastSelectedCampaignId`) en localStorage para futuros accesos.
- **Regla de Visibilidad Progresiva:** Los componentes analíticos descritos a continuación (Gráficos, Mapas de Calor, Tablas) están sujetos a una regla de Renderizado Condicional.
  - Solo se montan en el DOM si el usuario tiene actividad histórica (`recruitedCount > 0` o `role == 'ADMIN'`).
  - Para usuarios nuevos, ver estrategia de "Empty State" (RF-3.7-C).
  - **Disponibilidad por Fases:**
    - Los widgets de **Métricas Básicas** (Total Usuarios, Metas Individuales) son nativos de la Fase 1.
    - Los componentes de **Inteligencia Visual** (Mapa de Calor RF-7.1.D, Análisis de Penetración) corresponden a la **Fase 2**. Si el sistema se despliega en modo MVP, estos contenedores deben ocultarse o mostrar un estado "Recopilando Datos" hasta que haya volumen suficiente.

**A. KPIs de Rendimiento Transversales (Tarjetas Superiores):** Visibles para todos los roles de liderazgo, calculados sobre su territorio o rama asignada:

1. **Progreso de Meta (Contextual):** Gráfico tipo "Gauge" o Barra de Progreso.

- **Contexto A: Vista Estratégica (Coordinadores/Admin):** Mide la saturación del territorio.
    - **Fórmula:**  $(\text{Zone.stats.assignedVoters} / \text{Zone.stats.targetGoal}) * 100.$
  - **Contexto B: Vista Táctica (Multiplicadores/Enlaces):** Mide el desempeño individual (Incentivo Visual de Progreso).
    - **Fórmula:**  $(\text{user.metrics.recruitedCount} / (\text{user.personalGoal} || \text{system_config.goals.defaultMultiplierTarget})) * 100.$
    - **Lógica:** El sistema prioriza la meta personalizada del usuario. Si es null o 0, aplica automáticamente el estándar de campaña definido en la configuración global (ej: 1x10).
    - **Nota de Alcance:** El sistema utiliza técnicas de diseño motivacional (barras de progreso, medidores, códigos de color semánticos) para incentivar la acción. **NO** existe un sistema de acumulación de puntos canjeables ni recompensas tangibles en esta versión.
  - **Visual:** Código de color semántico (Rojo < 30%, Amarillo < 70%, Verde > 70%).
- 2. Velocidad de Crecimiento (Velocity): Comparativa diaria.**
- **Dato:** "Nuevos Hoy" vs. "Ayer".
  - **Indicador:** Flecha de tendencia (ej: +15% / ▼-5%).
- 3. Tasa de Conversión de Líderes:**
- **Fórmula:** (Usuarios con rol MULTIPLIER / Total Usuarios).
  - **Uso:** Indica qué tan activa es la base (no solo seguidores pasivos).
- 4. Usuarios Totales:** Conteo general de memberships activos.
- 5. Calidad del Voto (Embudo de Fidelización):**
- **Visualización:** Gráfico de barra apilada (Stacked Bar) o comparativo porcentual.
  - **Segmentos:**
    0.  **Simpatizantes:** (Total - Verificados). *Insight: "Trabajo por hacer".*
    1.  **Voto Fidelizado (Real):** Usuarios con `identityValidationStatus == 'VERIFIED'`. *Insight: "Caudal electoral seguro".*
  - **Objetivo Táctico:** Incentivar a los líderes a no solo "traer gente" (crecer la barra total), sino a "asegurar el voto" (convertir la barra gris en verde mediante validación).

**B. Variaciones de Interfaz por Rol (UI Especializada):** Para optimizar la operación, el sistema despliega widgets exclusivos según el perfil del usuario:

### 1. VISTA COORDINADOR (Perfil Estratégico / Auditor)

- **Alertas de Integridad (Widget Original):**

- **Indicador:** "Líderes en Revisión".
- **Filtro:** Usuarios donde fraudStatus != 'NORMAL'.
- **Acción:** Acceso directo a la lista de sus reclutados para realizar auditoría telefónica rápida (muestreo aleatorio).

- **Widget Financiero (Control de Presupuesto):**

- **Saldo de Comunicaciones:** Valor numérico del saldo disponible mostrado explícitamente en Dólares (ej: 120.50 USD). *Nota: No debe mostrarse el símbolo solo; debe acompañarse del código ISO USD para evitar confusión con COP.*
- **Burn Rate:** Gasto promedio diario en SMS/WhatsApp de los últimos 7 días.
- **Última Reconciliación:** Timestamp (Muestra al usuario cuándo corrió el "Sweeper" por última vez, generando confianza en el saldo mostrado).

- **Bandeja de Conflictos:** Lista de solicitudes de traslado pendientes ("Divorcios") para aprobación (RF-1.12).
- **Mapa de "Zonas Silenciosas":** Identificación de polígonos asignados con 0 registros en 7 días.

### 2. VISTA ENLACE (Perfil Táctico / Campo)

- **Top Movers del Día:** Ranking en tiempo real de sus 5 mejores Multiplicadores para gestión motivacional.
- **Alertas de Inactividad:** Semáforo Rojo para líderes que no han reportado en > 3 días.
- **Kit de Despliegue (Accesos Rápidos):**
  - Botón [GENERAR QR].
  - Botón [CERTIFICAR LÍDER] (Acceso a RF-3.11 para validación presencial).
- **Restricción:** Este rol NO visualiza el Widget Financiero ni las Alertas de Fraude complejas.

### 3. VISTA SEGUIDOR (Perfil Ciudadano / Base)

Interfaz diseñada para la retención, información logística y conversión (Ascenso). No muestra métricas de red ni herramientas de captura.

- **Credencial Digital (Header):**

- Datos: Foto (Avatar), Nombre Completo y Estado ("Verificado").
- Uso: Validación visual de pertenencia al movimiento en eventos presenciales.
- **Widget de Puesto de Votación (Logística Personal):**
  - **Si tiene puesto asignado:** Muestra Nombre del Puesto, Mesa, Dirección y un Mapa estático (Static API) con el pin de ubicación.
  - **Si no tiene puesto:** Muestra una alerta amarilla con el botón [ASIGNAR MI PUESTO] para completar el registro (Sujeto a reglas del RF-1.1).
- **Zona de Acción (Conversión):**
  - Componente Hero (Destacado): Botón "¿QUIERES SER LÍDER?".
  - Acción: Dispara el RF-1.4 (Protocolo de Ascenso). Al confirmar, el rol cambia a MULTIPLIER, se genera el QR y la interfaz se recarga mostrando el *Estado Vacío* (RF-3.7-C).
- **Canal de Noticias:** Acceso directo al WhatsApp oficial o video embebido de campaña.

## C. Gráficos Analíticos

- 1. Curva de Crecimiento:** Gráfico de Línea (Line Chart). Eje X: Últimos 30 días. Eje Y: Acumulado de registros.
- 2. Distribución por Rol:** Gráfico de Dona (Donut Chart). Segmentos: Multiplicadores vs. Seguidores vs. Enlaces.

## D. Métricas de Calidad de Datos (Preparación Día D)

- 1. Penetración Electoral (Votos por Puesto):** Listado o Mapa de Calor.
  - **Métrica:** Cantidad de usuarios agrupados por votingStationId.
  - **Uso:** Identificar puestos de votación donde la campaña es débil.
- 2. Completitud de Logística (Calidad de Datos Votante):**
  - **Dato:** % de Usuarios con Puesto de Votación Asignado vs. % Sin Puesto.
  - **Nota de Alcance:** Esta métrica mide la identificación del lugar de votación del ciudadano. La cobertura de testigos (Testigos vs. Mesas) es una métrica exclusiva del Dashboard de Fase 3 y no se mostrará en esta versión.

## E. Métricas Reservadas para Fase 3 (Hidden UI / Dark Features):

- Los siguientes indicadores, aunque puedan tener lógica de cálculo parcial en el backend, **NO DEBEN RENDERIZARSE** en el cliente en esta versión:
  - **Cobertura de Testigos:** (% de Mesas con Testigo Asignado).

- **Pre-Conteo Real:** (Total Votos Informados vs. Meta).
- **Avance de E-14:** (Fotos subidas vs. Total Mesas).
- **Justificación:** El sistema se encuentra en etapa de "Crecimiento y Estructura". Mostrar métricas de "Defensa del Voto" vacías genera ruido visual y desenfoque estratégico.

**RF-7.2: Política de Visibilidad Geográfica (Data Scoping)** El sistema filtra las consultas a la base de datos según el rol y la asignación territorial del usuario (`location.city` O `location.department`):

- **SUPER\_ADMIN:** Visibilidad Técnica Global (Logs, Configuración, Costos Proveedor).
- **ADMIN:** Visibilidad Operativa Global. Acceso a todas las métricas nacionales de la campaña, presupuesto operativo y auditoría de usuarios.
- **COORDINADOR:** Visualiza data donde `location.geoL1 == user.assignedGeoL1`.
- **ENLACE:** Visualiza data donde `location.geoL2 == user.assignedGeoL2`.
- **MULTIPLICADOR:** Visibilidad de **Rama**. Solo ve la data de las personas que él reclutó y su descendencia directa (Nietos/Bisnietos).
- **Principio de Auditoría Vertical (Inherited Oversight Policy):**
  - **Definición de Competencia:** En concordancia con la Estructura Jerárquica (Sección 2), se establece que **NO existen roles de auditoría aislados**. La facultad de inspeccionar logs de seguridad, validar alertas de fraude (RF-1.10) y revisar perfiles detallados es exclusiva del **Superior Jerárquico Directo**.
  - **Regla Técnica:** El sistema otorga permisos de auditoría sobre un usuario objetivo (Target) **SÍ Y SOLO SÍ** el UID del solicitante (Auditor) está presente en el array `hierarchyPath` del objetivo.
  - **Implicación Operativa:**
    - **El ADMIN:** Audita toda la campaña.
    - **El COORDINADOR:** Audita estrictamente los nodos dentro de su zona asignada. No puede auditar zonas vecinas (Silo de Datos).
    - **El ENLACE:** Audita la efectividad y veracidad de sus propios Multiplicadores.

**RF-7.5: Experiencia Móvil (Adaptive UI)** Interfaces adaptadas a móviles (Tarjetas en vez de tablas, Botones grandes, Bottom Bar).

## RF-7.6: Motor de Búsqueda Omnipresente (Server-Side Prefix Search)

Componente de interfaz disponible en la cabecera que permite la localización rápida de registros mediante consultas indexadas nativas, respetando estrictamente los permisos de visualización.

### A. Estrategia de Indexación (Firestore Native):

- **Limitación Técnica:** Debido a la restricción de costos (RNF-7), NO se utilizan motores de búsqueda de texto completo (como Algolia) ni librerías pesadas en cliente (Fuse.js) para el dataset global.

- **Alcance del Índice (Scope Restriction):**

- La búsqueda se ejecuta estrictamente sobre la colección raíz /users (**Scope: COLLECTION**).
- **Prohibición:** No se realizan búsquedas globales ("Cross-Collection"). El motor de búsqueda aplica los filtros de seguridad (RF-7.2) aprovechando los índices compuestos hierarchyPath + searchKey para garantizar que un usuario solo encuentre registros dentro de su propia rama o zona, optimizando la lectura de documentos.

- **Mecanismo:** La búsqueda funciona exclusivamente bajo lógica "**Starts With**" (Prefijo).

- **Campo Espejo (searchKey):**

- **Algoritmo de Normalización (Canonicalización):**

- Se utiliza el estándar **Unicode NFD** para descomponer grafemas.
- **Función Técnica:** str.normalize("NFD").replace(/[\u0300-\u036f]/g, "").toLowerCase().
- **Efecto:** Elimina diacríticos (á -> a) y simplifica caracteres complejos (ñ -> n, ü -> u) para maximizar la coincidencia en búsquedas rápidas (Recall).

- **Indexación de Alias (Política de Apodos):**

- Dado que en política local es común buscar por sobrenombre, el searchKey se construye concatenando: normalizedFullName + " " + normalizedAlias.
- *Ejemplo:*
  - Nombre: "José Antonio Gómez"
  - Alias: "Toño"
  - **searchKey Resultante:** "jose antonio gomez tono"
- *Beneficio:* El usuario puede buscar "Toño" y el sistema encontrará el registro correctamente.

**B. Criterios de Búsqueda Soportados:** El sistema debe admitir consultas por los siguientes identificadores:

1. **Cédula (documentId):** Búsqueda exacta. Prioridad Alta.
2. **Código QR (sourceQr):** Búsqueda exacta (ej: "M-001"). Útil para validar identidad física.
3. **Teléfono (phone):** Búsqueda exacta (últimos 10 dígitos).
4. **Nombre (fullName):** Consulta de rango sobre searchKey (startAt/endAt).

**C. Filtro de Seguridad (Scope Enforcement):**

- **Restricción Mandatoria:** Los resultados de la búsqueda **NO son globales**. El motor aplica una intersección obligatoria con los permisos del usuario (RF-7.2).
- **Regla de Negocio (Scope Enforcement):**
  - El sistema añade automáticamente la cláusula .where('hierarchyPath', 'array-contains', user.uid) a cualquier búsqueda realizada por un Multiplicador.
  - Esto garantiza que, incluso si una rama crece horizontalmente a miles de usuarios, la búsqueda se ejecute dentro de los límites de los índices compuestos sin exceder cuotas de memoria ni tiempos de ejecución.

- Si un **Coordinador** busca, solo ve resultados cuya location.city o zone coincide con su jurisdicción asignada.
- **Implementación Técnica:** Toda Query de búsqueda debe incluir cláusulas .where() compuestas que validen el uid o zonel del solicitante antes de ejecutar el filtro de texto.
- **Dependencia de Infraestructura:** La ejecución eficiente de estas consultas (filtro de permisos + búsqueda de texto) depende estrictamente de la existencia de los índices compuestos "Búsqueda en Rama" y "Búsqueda en Zona" definidos en el **RF-4.4**.
  - *Restricción:* Si estos índices no están desplegados, el sistema arrojará un error de índice faltante en lugar de realizar un escaneo completo de la colección, protegiendo así la cuota de lectura (Cost-Saving).

**RF-7.7: Estrategia de Carga de Listas (Virtual Infinite Scroll)** Para cumplir con los requisitos de rendimiento móvil (RNF-1) y optimización de costos de lectura en Firestore, todas las vistas de listado (Seguidores, Auditoría, Logs) deben implementar el siguiente protocolo:

#### A. Backend (Firestore - Cursor Pagination):

- **Prohibición:** Queda estrictamente prohibido realizar consultas abiertas (collection.get()) sin cláusula limit().
- **Lógica de Consulta:**
  1. **Batch Size:** Se solicitan bloques de **50 documentos** máximo por llamada.
  2. **Paginación:** Se utiliza el método startAfter(lastVisibleDocument) para obtener el siguiente bloque, evitando el uso de offset (que es ineficiente en NoSQL).

#### B. Frontend (Virtualization & Windowing):

- **Tecnología:** Implementación de **Virtual Scrolling** (ej: TanStack Virtual o React Virtuoso).
- **Comportamiento:** El navegador solo renderiza en el DOM los elementos visibles en la ventana gráfica (viewport) + un buffer pequeño (ej: 10 items).

- **Efecto:** Aunque la lista cargada tenga 5,000 registros en memoria JS, el navegador solo "pinta" 15 filas, manteniendo los 60FPS en el scroll.
- **Disparador de Carga:** Un observador (IntersectionObserver) al final del scroll dispara automáticamente la petición del siguiente bloque de 50 registros.

**RF-7.8: Generación de Listados de Punteo (Print-Ready Export)** Herramienta de materialización de datos para operaciones en zonas con conectividad nula o gestión manual.

- **Tecnología (Client-Side):** Implementación de hoja de estilos específica de impresión (@media print). El usuario utiliza la función nativa del navegador "Imprimir -> Guardar como PDF".
- **Diseño "Eco-Ink":**
  - Al activar el modo impresión, la interfaz elimina: Barras de navegación, mapas, colores de fondo y avatares.
  - Se fuerza tipografía negra sobre fondo blanco 100%.
  - Se ajusta el tamaño de fuente a 10pt para maximizar registros por hoja (A4/Carta).
- **Formato de Planilla (Checklist):** La tabla se reestructura automáticamente para mostrar:
  1. **Identificación:** Nombre y Últimos 4 dígitos de Cédula.
  2. **Logística:** Puesto de Votación y # de Mesa.
  3. **Contacto:** Teléfono.
  4. **Columna de Acción:** Casilla vacía [ ] encabezada como "VOTÓ".

- **Seguridad del Papel:**
  1. El pie de página de cada hoja impresa incluye automáticamente: "Generado por [UID Usuario] el [Fecha/Hora]. Documento Confidencial de Campaña."
  2. **Objetivo:** Trazabilidad en caso de que una lista se pierda o filtre.

## RF-7.9: Estrategia de Caché y Eficiencia de Lectura (Data Fetching Policy)

- **Problema:** El uso de oyentes en tiempo real (onSnapshot) en tableros con miles de usuarios concurrentes multiplica los costos de lectura de Firestore exponencialmente (1 cambio en BD = N lecturas en clientes conectados), violando el RNF-7.
- **Estrategia Técnica:** Se implementa el patrón **SWR (Stale-While-Revalidate)** para todas las consultas de lectura en el Dashboard (GET).
- **Reglas de Tiempos de Vida (Cache TTL):**

0. **KPIs y Gráficos (Agregados):** Se establece un intervalo de deduplicación de **5 Minutos**.

- *Efecto:* Si el usuario navega entre pestañas o recarga la página dentro de este periodo, el sistema sirve los datos de la memoria local sin tocar la base de datos.

1. **Listados Operativos:** Intervalo de **60 Segundos**.

- *Efecto:* Permite la navegación fluida "Atrás/Adelante" en listas de seguidores sin re-facturar la consulta.

2. **Disparadores de Revalidación (Mutaciones):** La caché se invalida y refresca forzosamente **solo** cuando el usuario realiza una acción de escritura explícita (ej: Registrar un Votante, Aprobar un Traslado), garantizando que el usuario siempre vea el resultado inmediato de sus propias acciones.

- **Restricción de Implementación:** Queda **prohibido** el uso de suscripciones en tiempo real (firestore.collection(...).onSnapshot) para métricas globales o listados masivos. Su uso se reserva estrictamente para objetos individuales críticos en flujos de edición (ej: Documento de Zona activa).

## RF-7.10: Tablero de Resultados de Mensajería (Engagement Metrics)

El sistema debe renderizar los datos almacenados en responseDistribution utilizando:

- **Embudo de Conversión:** Visualización comparativa de sent -> read -> replied.

- **Distribución de Opinión:** Gráfico de Donas o Barras basado en las claves del mapa responseDistribution.

## 4.8 MÓDULO 8: SEGURIDAD Y ACCESO

### RF-8.1: Autenticación Simplificada y Seguridad

- **Tecnología Base:** Auth.js (Ecosistema NextAuth).

- **Métodos Soportados:**

- **Passwordless/OTP:** SMS y WhatsApp.
- **Social Providers:** Google, Facebook, Twitter.
- **Credenciales:** Email + Password (Hash seguro).

- **Integridad de Sesión:**

- Se mantiene la **Política de Dispositivos (Device Cap)** y el **Security Kill-Switch** (RF-8.9) descritos originalmente.
- Se mantiene el **Manejo de Sesión Offline** (RF-3.5) para garantizar el funcionamiento de la PWA sin red.
- **Account Linking:** El sistema debe tratar de unificar cuentas si detecta el mismo email o teléfono verificado proveniente de distintos proveedores.

- **Política de Selección de Versión (Estabilidad Crítica):**

- **Mandato Técnico:** Se establece **NextAuth.js v4 (LTS)** como la versión obligatoria y definitiva para el desarrollo de la Fase 1 y 2.
- **Justificación:** La operación electoral tiene una fecha límite inamovible ("Día D"). La campaña no puede asumir el riesgo de inestabilidad, falta de documentación o cambios rupturistas (*Breaking Changes*) asociados a la versión v5 (Beta/Experimental). La confiabilidad del acceso prevalece sobre la novedad tecnológica.
- **Adaptación a App Router:** Dado que v4 requiere configuración específica para funcionar con el Middleware de Next.js App Router, el equipo de desarrollo debe implementar el patrón de **Configuración**

**Segregada** (separar auth.config.ts de la lógica de base de datos) para garantizar la compatibilidad con el entorno *Edge*, en lugar de esperar el soporte nativo de v5.

- **Mecanismo de Acceso e Integridad de Sesión (Mobile Context Guard):**

- **Política de "Código Primero" (Code-Over-Link):** Para evitar que los enlaces de acceso abran navegadores externos y desconecten al usuario de su base de datos local (PWA/IndexedDB), se aplica la siguiente lógica según el dispositivo:
  - **En Móviles (Mandatorio):** La interfaz **fuerza** el uso de un Código de Un Solo Uso (**OTP**) manual.
    - *Canal SMS/WhatsApp:* Envío estándar de código numérico (Sujeto a costos RF-5.6).
    - *Canal Email:* En lugar de un enlace clicable ("Magic Link"), el sistema envía un "**Magic Code**" visual (ej: "Tu código de acceso es: **892-123**") para que el usuario lo copie y pegue en la App.
  - **En Desktop:** Se permite el uso híbrido de Magic Link (clic directo) o Código, según preferencia del usuario.
- **Excepción Técnica (Deep Linking):** El uso de enlaces de autologin en móviles solo se habilita si se implementan protocolos de *Universal Links/App Links* verificados que garanticen la apertura forzada dentro de la PWA instalada. De lo contrario, el sistema hace *fallback* automático al modo OTP.

- **Protocolo de Recuperación Autoservicio (Self-Service Recovery):**

- **Alcance:** Disponible exclusivamente para usuarios que tengan un **Email Verificado** asociado a su cuenta o que usen autenticación por Contraseña.
- **Mecanismo (Magic Code via Email):**
  - El usuario solicita "Recuperar Cuenta" en el Login.
  - El sistema envía un código numérico de 6 dígitos al correo registrado (TTL: 10 minutos).

- **Acción:** Al ingresar el código correcto en la PWA, el sistema permite establecer una nueva contraseña (si aplica) o iniciar sesión directamente.

- **Excepción:** Si el usuario **NO** tiene email registrado y perdió su acceso telefónico (SIM Card), el sistema lo deriva obligatoriamente al **Flujo Manual con Coordinador** (ver RF-1.7).

#### RF-8.2: Matriz de Control de Acceso (RBAC) Segregación estricta de permisos.

| Función               | SUPER_ADMIN             | Admin                        | Coord        | Enlace    | Mult | Seguidor |
|-----------------------|-------------------------|------------------------------|--------------|-----------|------|----------|
| Generar QRs           | ✗                       | ✓                            | ✓            | ✓         | ✓    | ✗        |
| Ver Dashboard         | Global (Sistema)        | Global (Campaña)             | Departamento | Municipio | Rama | Personal |
| Exportar Excel        |                         | ✓ (DLP)                      | ⊖            | ⊖         | ⊖    | ⊖        |
| Importar CSV (Masivo) | ✓ (Datos voting_places) | ✓ (Datos de usuarios, votos) | ✗            | ✗         | ✗    | ✗        |
| Crear Campaña SMS     | ✗                       | ✓                            | ✓ (\$)       | ✓ (\$)    | ✗    | ✗        |

| Función                   | SUPER_ADMIN                                              | Admin                                                  | Coord                                           | Enlace                                            | Mult                                       | Seguidor                                   |
|---------------------------|----------------------------------------------------------|--------------------------------------------------------|-------------------------------------------------|---------------------------------------------------|--------------------------------------------|--------------------------------------------|
| Recargar Saldo            | <input checked="" type="checkbox"/> (Corrección técnica) | <input checked="" type="checkbox"/> (ACL) <sup>1</sup> | <input checked="" type="checkbox"/>             | <input checked="" type="checkbox"/>               | <input checked="" type="checkbox"/>        | <input checked="" type="checkbox"/>        |
| Editar Puesto Votación    | <input checked="" type="checkbox"/>                      | <input checked="" type="checkbox"/>                    | <input checked="" type="checkbox"/>             | <input checked="" type="checkbox"/>               | <input checked="" type="checkbox"/> (Self) | <input checked="" type="checkbox"/> (Self) |
| Reasignación Masiva       | <input checked="" type="checkbox"/>                      | Total                                                  | Solo sub Rama                                   | <input checked="" type="checkbox"/>               | <input checked="" type="checkbox"/>        | <input checked="" type="checkbox"/>        |
| Aprobar "Divorcios"       | <input checked="" type="checkbox"/>                      | <input checked="" type="checkbox"/>                    | <input checked="" type="checkbox"/>             | <input checked="" type="checkbox"/>               | <input checked="" type="checkbox"/>        | <input checked="" type="checkbox"/>        |
| Validar Alerta Fraude     | <input checked="" type="checkbox"/>                      | <input checked="" type="checkbox"/>                    | <input checked="" type="checkbox"/>             | <input checked="" type="checkbox"/>               | <input checked="" type="checkbox"/>        | <input checked="" type="checkbox"/>        |
| Ver Mapa Completo         |                                                          | <input checked="" type="checkbox"/>                    | <input checked="" type="checkbox"/> (Polígonos) | <input checked="" type="checkbox"/> (Solo Puntos) | <input checked="" type="checkbox"/>        | <input checked="" type="checkbox"/>        |
| Promover Roles (Staffing) | <input checked="" type="checkbox"/>                      | <input checked="" type="checkbox"/>                    | <input checked="" type="checkbox"/>             | <input checked="" type="checkbox"/>               | <input checked="" type="checkbox"/>        | <input checked="" type="checkbox"/>        |

#### RF-8.3: Cumplimiento Legal y Anonimización (Derecho al Olvido)

Configuración adaptable para Ley 1581 (Colombia) o GDPR.

<sup>1</sup> (ACL) Requiere validación secundaria contra la lista 'financialAdmins' en la configuración global.

- **Estrategia de Borrado:** No se realiza un borrado físico del documento (delete()) para evitar la orfandad de los nodos hijos (referencias rotas en parentId).
- **Política de Persistencia en Copias de Seguridad (Cold Storage Exception):**
  - **Limitación Técnica:** La anonimización se ejecuta sincrónicamente solo en la Base de Datos Operativa (Hot Storage). Los registros contenidos en los archivos de Backup (GCS) **NO** son modificados ni eliminados en el acto debido a su naturaleza inmutable.
  - **Cumplimiento Diferido:** Estos datos históricos permanecen latentes hasta que el archivo de respaldo alcanza su ciclo de vida automático (30 días, ver RF-8.6) y es eliminado permanentemente por el sistema.
  - **Cláusula de No-Procesamiento:** Durante este periodo de latencia (ventana de 30 días), los datos en backup se consideran legalmente "Fuera de Uso" (Beyond Use) y no están sujetos a tratamiento activo, cumpliendo con el principio de finalidad de la Ley 1581.
  - **Protocolo de Restauración:** Si ocurriese un desastre que obligue a restaurar un backup antiguo, el Admin asume la responsabilidad de volver a ejecutar manualmente los procesos de anonimización pendientes que hayan ocurrido en el intervalo perdido.
- **Sobrescritura Destructiva (Data Scrubbing):** Al confirmar una solicitud de baja, el sistema ejecuta una actualización masiva sobre el documento del usuario:
  - **Identificadores Personales:** fullName se sobrescribe con "USUARIO ELIMINADO". phone y address se establecen en null o cadenas vacías.
  - **Cédula (Unique Index):** Para liberar la cédula real (permitiendo un registro futuro si el usuario regresa) y evitar colisiones en el índice único, el documentId se reemplaza por un hash único de descarte: deleted\_[TIMESTAMP]\_[RANDOM].
  - **Integridad Estructural:** Se conservan el uid (ID del documento), el parentId y las métricas históricas (recruitedCount), permitiendo que la red siga existiendo visualmente, aunque el nodo sea anónimo.

- **Credenciales:** Se revoca y elimina el acceso en el proveedor de identidad (Auth.js/Firebase Auth).
- **Excepción de Integridad Financiera y Auditoría (Immutable Ledger Policy):**
  - **Limitación del Alcance:** El proceso de "Sobrescritura Destructiva" se aplica **exclusivamente** al documento del perfil de usuario en la colección users.
  - **Protección de Libros:** Las colecciones wallet\_transactions (RF-4.2.D) y audit\_logs (RF-4.2.C) están **exentas** de modificación o anonimización.
  - **Justificación Técnica y Legal:**
    - Dado que el sistema mantiene el UID del usuario (bajo la regla de "Integridad Estructural" definida arriba), los registros históricos en los libros contables no quedan huérfanos; apuntan válidamente a un registro que ahora se visualiza como "USUARIO ELIMINADO".
    - Esto garantiza el cumplimiento de las normas fiscales que exigen conservar soportes de transacciones (Recargas y Gastos) por tiempos superiores a la permanencia del usuario en la plataforma, sin violar el Habeas Data (ya que el perfil público ha sido suprimido).

**RF-8.5: Seguridad Infraestructura (WAF)** Implementación de Google Cloud Armor para protección contra ataques DDoS y filtrado de tráfico malicioso.

**RF-8.6: Estrategia de Continuidad de Negocio (Backup & Recovery)** Protocolo de protección contra pérdida de datos, corrupción o borrado accidental (Human Error).

- **1. Recuperación Granular (PITR - Point-in-Time Recovery):**
  - *Tecnología:* Firestore Native PITR.
  - *Ventana:* **7 Días móviles.**

- *Función:* Permite restaurar la base de datos (o documentos específicos) a su estado exacto en cualquier minuto del pasado reciente.
- *Caso de Uso:* "El Coordinador borró sin querer la Zona Norte hace 15 minutos". Solución: Revertir el estado de la colección a T - 20 min.

- **2. Copias de Seguridad Programadas (Cold Storage):**

- *Frecuencia:* Diaria (03:00 AM America/Bogota).
- **Configuración:** El trabajo de *Cloud Scheduler* debe tener configurado explícitamente el parámetro *timeZone*: 'America/Bogota' para garantizar que la copia ocurra durante la madrugada colombiana, independientemente de si el servidor de Cloud Run está alojado en us-central1 o europe-west1.
- *Mecanismo:* Cloud Scheduler activa un trabajo de exportación a **Google Cloud Storage (Bucket Regional)**.
- *Retención:* Ciclo de vida de 30 días (los backups antiguos pasan a clase "Archive" para reducir costos o se eliminan).
- *Formato:* BSON/JSON comprimido.

- **3. Protocolo de Restauración (Restricción de Mando):**

- La acción de "Restaurar Backup" está bloqueada por defecto en el Dashboard. Requiere autenticación de dos factores (2FA) y rol exclusivo de **SUPER\_ADMIN (Soporte Técnico)**. El rol **ADMIN** (Campaña) no tiene permisos para sobrescribir la base de datos completa.

- **4. Protocolo de Reversión Inmediata (Instant Rollback - Cloud Run):**

- **Política de Despliegue:** Durante la semana electoral (Semana Crítica), se prohíbe la estrategia de "Reemplazo de Revisión". Se debe utilizar **Traffic Splitting**.
- **Mecanismo:**
  - La versión estable (v0.5) se mantiene activa con 0% de tráfico.

- Si la nueva versión (v1.0) presenta fallos críticos (Error Rate > 1%), el Administrador ejecuta un comando de emergencia en GCP Console para redirigir el 100% del tráfico a la revisión estable anterior.
- **Tiempo de Recuperación (RTO):** < 30 segundos (sin necesidad de recompilar código).

### RF-8.7: Control de Tasa y Protección contra Abuso SMS (Rate-Limiting)

Se implementa una estrategia de defensa en profundidad (Application Layer + Network Layer) para prevenir costos excesivos y ataques de fuerza bruta sobre el servicio de OTP.

#### A. Reglas de Negocio (Application Layer - Middleware):

Se configuran límites estrictos asociados al identificador del usuario (Teléfono) y su huella digital.

| Métrica                           | Límite           | Acción al Exceder                                                                                          |
|-----------------------------------|------------------|------------------------------------------------------------------------------------------------------------|
| <b>Cooldown entre Envíos</b>      | 60 Segundos      | Botón "Reenviar Código" deshabilitado visualmente (UI) y bloqueado en API. Muestra cuenta regresiva.       |
| <b>Límite por Teléfono (Hora)</b> | 5 Intentos       | Bloqueo temporal por 1 hora. Mensaje: "Demasiados intentos. Intenta más tarde."                            |
| <b>Límite por Teléfono (Día)</b>  | 10 Intentos      | Bloqueo por 24 horas. Requiere intervención de Soporte/Admin para desbloqueo manual.                       |
| <b>Validación Fallida</b>         | 3 Errores de OTP | El código OTP actual se invalida inmediatamente. Se fuerza a solicitar uno nuevo (respetando el cooldown). |

#### B. Reglas de Infraestructura (Google Cloud Armor):

Protección basada en IP para evitar ataques desde botnets o redes anónimas.

- **Throttling por IP:** Máximo 20 solicitudes de login (/api/auth/signin) por minuto desde la misma IP.

- *Excepción:* Se debe configurar una lista blanca (Allowlist) para la IP de la Sede Central de Campaña (HQ campaign.settings.security.hqWhitelistedIps), donde múltiples usuarios legítimos comparten la misma conexión WiFi.
- **Protocolo de Lista Blanca Dinámica (HQ Whitelist):**

- **Definición:** El sistema debe permitir la exclusión de direcciones IP específicas de las reglas de *Rate Limiting* para garantizar la operación en sedes de campaña (donde 50+ usuarios comparten una IP pública).
- **Gestión:** Esta lista NO es estática en código. Debe ser editable desde el Dashboard de Administración (guardada en system\_config).
- **Lógica de Bypass:** Antes de aplicar el bloqueo por frecuencia, el Middleware consulta la lista de IPs permitidas en caché. Si hay coincidencia, el contador de solicitudes se ignora.
- **Seguridad:** Las IPs en lista blanca siguen sujetas a validación de tokens (Auth), solo se eximen del límite de frecuencia.

- **Geobloqueo:** Se bloquea el tráfico proveniente de países fuera del territorio electoral (ej: permitir solo tráfico de Colombia + USA/España si hay comités en el exterior).

### C. Alertas de Anomalía:

Si el sistema detecta > 50 fallos de OTP consecutivos a nivel global en < 5 minutos, se activa el "Modo Bajo Ataque":

1. Se detiene el servicio de SMS temporalmente.
2. Se notifica al Admin vía Email.
3. El login comuta a modo "Solo Password" (si existe) o muestra mensaje de mantenimiento.

**RF-8.8: Protocolo de Auditoría de Lectura (The Silent Watcher)** Mecanismo de disuasión y control que registra el acceso a información sensible, incluso si no se realizan cambios en los datos.

**A. Disparador del Evento (Trigger):** Se genera un registro de auditoría automáticamente cuando:

1. Un usuario con rol administrativo (Admin, Coord, Enlace) abre la vista de **Detalle Completo** (/dashboard/user/[UID]) de un tercer persona.
2. **Excepción:** No se genera log si el usuario está viendo su propio perfil (ViewerID == TargetID).

**B. Detección de Anomalías (Scraping Manual):** El sistema monitorea la velocidad de generación de estos logs.

- **Patrón de Alerta:** Si un mismo usuario genera > 20 eventos VIEW\_PROFILE en < 1 minuto.
- **Acción:** Se marca la cuenta preventivamente como SUSPICIOUS\_ACTIVITY y se notifica al Admin. Esto sugiere que el usuario está "minando" datos manualmente o usando un script de scraping.

**C. Política de Retención:** Debido al alto volumen potencial de estos logs de lectura, su ciclo de vida en la base de datos "caliente" (Firestore) es de solo **30 días**. Posteriormente, se exportan a Cold Storage (BigQuery/GCS) y se eliminan de la vista operativa para ahorrar costos.

**RF-8.9: Política de Concurrencia y Gestión de Dispositivos** Define las reglas para el manejo de múltiples sesiones simultáneas (Auth Tokens) bajo un mismo UID.

**A. Límite de Dispositivos (Device Cap):**

- **Regla:** Se permite un máximo de **3 sesiones activas** (Refresh Tokens válidos) por usuario simultáneamente.
- **Estrategia de Rotación (FIFO):** Si un usuario inicia sesión en un 4º dispositivo, el sistema revoca automáticamente el token de la sesión **más antigua** (Last Active).
  - **UX:** El dispositivo viejo recibirá un error 401 y mostrará: "Tu sesión se cerró porque ingresaste en otro dispositivo."

**B. Protocolo de Invalidación por Cambio de Rol (Security Kill-Switch):** Para garantizar que los cambios de jerarquía surtan efecto inmediato y prevenir accesos no autorizados tras un despido o democión.

- **Disparador:** Cualquier actualización en el campo role de la colección users (ej: De COORDINATOR a FOLLOWER).
- **Acción:** El backend (Cloud Function) busca y **revoca todas** las sesiones activas asociadas a ese UID en la tabla de autenticación.
- **Efecto:** El usuario es expulsado forzosamente de todos sus dispositivos y debe volver a iniciar sesión (obteniendo un nuevo token con los permisos reducidos).

**C. Autogestión de Seguridad (User Control):** En la vista "Mi Perfil", el usuario debe visualizar un panel de "**Dispositivos Activos**:

- Lista: Tipo de dispositivo (User Agent simplificado), IP, y "Última vez activo".
- Acción: Botón **[Cerrar sesión en otros dispositivos]** para proteger su cuenta en caso de pérdida o sospecha.

**D. Ciclo de Vida de la Sesión (Token TTL Policy):** Se define una política de caducidad para evitar sesiones "zombis" indefinidas, equilibrando la seguridad con la operatividad offline.

- **Access Token (Corto Plazo):**

- **TTL:** 1 Hora.
- **Propósito:** Credencial efímera para transacciones API. Su caducidad breve minimiza el riesgo si se intercepta el tráfico.

- **Refresh Token (Largo Plazo - Persistencia):**

- **TTL Base: 30 Días.**
- **Mecanismo de Rotación (Rolling Window):** Cada vez que el sistema renueva un Access Token exitosamente (uso activo de la App), se emite un *nuevo* Refresh Token y el contador de 30 días se reinicia.
- **Hard Stop (Caducidad por Inactividad):** Si el usuario **NO** abre la aplicación durante 30 días consecutivos, el token vence definitivamente.

- **Acción:** El sistema cierra la sesión y exige re-autenticación vía OTP.
- **Manejo de Expiración Offline (Integración con RF-3.5):** \* Si el token caduca mientras el dispositivo está sin conexión (ej: el usuario abre la app tras 35 días sin uso y sin internet), se activa el estado **PAUSED\_AUTH\_REQUIRED** definido en el **RF-3.5**. \* **Protección de Datos:** La interfaz bloquea la navegación, pero **NO elimina** los formularios pendientes de sincronizar en IndexedDB. Se permite al usuario hacer re-login cuando recupere señal para transmitir su trabajo guardado.

**RF-8.10: Gestión Centralizada de Secretos (Zero-Trust Credentials)** Protocolo para el manejo seguro de llaves de API y credenciales de servicio, evitando su exposición en repositorios o variables de entorno visibles.

- **Tecnología:** Uso obligatorio de **Google Secret Manager**.
- **Implementación en Producción:**
  - El servicio de Cloud Run NO recibe las llaves como variables de entorno (ENV\_VARS) legibles en la consola de GCP.
  - En su lugar, se inyectan como volúmenes montados o se acceden vía SDK usando la Identidad del Servicio (Service Account Identity).
- **Inventario de Secretos Protegidos:**
  1. TWILIO\_AUTH\_TOKEN: Acceso a gastos financieros.
  2. FIREBASE\_ADMIN\_KEY: Acceso total a la base de datos (Service Account).
  3. Maps\_SERVER\_KEY: API Key de Geocodificación (Backend).
  4. AUTH\_SECRET: Llave de encriptación de sesiones de Auth.js.
- **Rotación:** El sistema debe soportar el cambio de estas llaves sin requerir un nuevo despliegue de código (Redeploy), simplemente reiniciando la instancia para refrescar el secreto en memoria.

**RF-8.11: Política de Retención y Archivado de Logs (Data Lifecycle Policy)**

- **Justificación:** Garantizar la sostenibilidad del sistema (RNF-7) evitando el crecimiento indefinido de la colección audit\_logs en la base de datos transaccional, sin perder la evidencia histórica requerida legalmente.

- **Nivel 1: Operación Activa (Hot Storage):**

- **Ubicación:** Colección audit\_logs en Firestore.
- **TTL (Time-to-Live): 180 Días (6 Meses).**
- **Propósito:** Permite la consulta inmediata desde el Dashboard para auditoría de campaña, resolución de disputas de pagos y monitoreo de seguridad en tiempo real.

- **Nivel 2: Archivo Histórico (Cold Storage):**

- **Mecanismo:** Se configura una *Cloud Function* programada (Scheduler) o un disparador de evento que exporta los documentos por vencer hacia **Google Cloud Storage (Clase Archive)** antes de su eliminación.
- **Formato:** JSON comprimido (NDJSON/GZIP) organizado por año/mes.
- **Retención Legal:** Estos archivos inmutables se conservan por un periodo mínimo de **5 años** (o lo que exija la normativa electoral local) para análisis forense bajo demanda, pero ya no consumen recursos de la base de datos activa.

#### **RF-8.12: Pipeline de Despliegue Seguro (CI/CD Zero Trust)**

Estrategia de automatización para el despliegue continuo en Google Cloud Run eliminando vectores de ataque por robo de credenciales estáticas.

- **Tecnología de Autenticación:** Se implementa **Workload Identity Federation (WIF)** para conectar GitHub Actions con Google Cloud.

- **Mecanismo:** El proveedor de identidad de GitHub (OIDC) intercambia un token firmado por un token de acceso de Google Cloud de corta duración (TTL < 1 hora) en tiempo de ejecución.
- **Restricción Mandatoria (Keyless Policy):** Queda estrictamente **PROHIBIDO** generar, descargar o almacenar archivos

de claves de cuenta de servicio (service-account-key.json) en los Secretos del repositorio.

- **Segregación de Privilegios en Despliegue:**

- El pipeline debe utilizar dos Cuentas de Servicio (SA) distintas configuradas en el WIF, respetando la segregación de entornos del **RNF-8**:
  0. sa-deploy-staging@project.iam.gserviceaccount.com: Solo tiene permisos para desplegar en la revisión de pruebas.
  1. sa-deploy-prod@project.iam.gserviceaccount.com: Solo tiene permisos para desplegar en el servicio de producción.

- **Condición de Integridad:** El WIF debe configurarse para confiar únicamente en el repositorio oficial de la organización y, para el entorno de producción, restringir el despliegue exclusivamente a la rama main o tags firmados.

---

## 5. REQUERIMIENTOS NO FUNCIONALES

- **RNF-1 Performance:** Carga de formulario PWA < 2 segundos en 3G. Dashboard móvil con interactividad inmediata.
- **RNF-2 Escalabilidad:** Arquitectura elástica (Cloud Run + Firestore). Soporte de picos 10x tráfico electoral.
- **RNF-3 Disponibilidad y Resiliencia:** Offline-First (Operación sin señal 72h). Fallback automático de Mapas. Tolerancia a Fallos de Sesión: El sistema debe ser capaz de retener datos en cola local indefinidamente si la sesión caduca, prohibiendo el descarte de datos (Data Loss) por errores de autenticación 401.

- **Gestión de Dependencia de Proveedores (SPOF & Service Continuity Strategy):**

- **Arquitectura Single-Vendor (v1.0):** Se establece explícitamente que el sistema opera bajo dependencia exclusiva de **Twilio** para los servicios de mensajería

(SMS/WhatsApp). **NO** existe comutación automática (Failover) a proveedores secundarios.

- *Justificación Técnica:* La portabilidad de plantillas de WhatsApp (BSP Lock-in) y la integridad del cálculo de costos centralizado (RF-5.6) impiden el cambio dinámico de ruta.

- **Protocolo de Contingencia (Queue & Retry Policy):**

- **Envíos Masivos:** Ante un fallo global del proveedor, la cola de mensajería (Cloud Tasks definida en RF-5.1) entrará en modo de **Retención (Exponential Backoff)**, reintentando la entrega por hasta 72 horas. No se pierden mensajes, solo se retrasan.
- **Acceso (Login OTP):** Se acepta una degradación de servicio. Si Twilio cae, el ingreso vía SMS se detendrá. Se instruye el uso de mecanismos alternativos (Magic Code vía Email) o el soporte en sesiones activas (que no requieren OTP gracias al Refresh Token de 30 días del RF-8.9).
- **Continuidad del Negocio:** La funcionalidad crítica de **Captura de Votos (RF-1.1)** opera de forma totalmente independiente (Offline-First). La caída del servicio de mensajería **NUNCA** detiene la capacidad de la campaña para registrar nuevos simpatizantes.

- **RNF-4 Usabilidad y Accesibilidad Visual (Sunlight-Ready):**

- **Mobile-first:** Diseño responsive (Tailwind CSS).
- **Autenticación Passwordless**
- **Contraste para Exteriores:** La interfaz debe cumplir estrictamente con el estándar **WCAG AA** (Ratio 4.5:1 mínimo).

- *Restricción:* Se prohíbe el uso de texto gris claro o colores pastel en información crítica (Nombres, Cédulas, Alertas).
  - *Justificación:* Garantizar la legibilidad de la pantalla bajo **luz solar directa** durante el barrido territorial.
- **Interacción Física:** Áreas de toque (Touch Targets) mínimas de **48x48px** para facilitar el uso mientras se camina.

- **Adaptabilidad de Marca (Dynamic Theming):**

- La interfaz debe aplicar los colores definidos en political\_campaigns.branding utilizando Variables CSS (ej: --primary-color).
- **Salvaguarda de Contraste:** Si el color primario configurado por el Admin es muy claro (Luminosidad > 80%), el sistema debe forzar automáticamente el color de texto de los botones a negro (#000) en lugar de blanco (#FFF) para cumplir WCAG AA.

- **RNF-5: Optimización Diferencial de Medios** Estrategia de compresión adaptativa según el valor legal de la imagen:

- **Avatares y Perfiles:** Compresión agresiva (WebP < 150KB). Prioridad: Velocidad de carga.
- **Evidencia Legal (E-14) [SOLO FASE 3]:** Modo "Alta Fidelidad".
  - **Formato:** WebP con quality: 0.85 (Lossy High Quality).
  - **Límite:** Máximo **3 MB** por fragmento.
  - **Justificación:** La legibilidad de los dígitos manuscritos prevalece sobre el costo de almacenamiento. El sistema de "Carga Resiliente" (RF-3.9) gestionará la subida de estos archivos más pesados mediante fragmentación.

- **RNF-6: Matriz de Compatibilidad y Hardware Soportado** Para garantizar el funcionamiento crítico de los módulos de Escaneo QR (RF-2), Mapas (RF-6) y Notificaciones, los dispositivos de los líderes deben cumplir con los siguientes mínimos:

- **A. Sistema Operativo (OS):**

- **Android:** Versión **8.1 (Oreo)** o superior.
  - *Requisito Crítico:* Navegador Chrome o Edge actualizado (Motor Chromium v100+). No se garantiza soporte en navegadores nativos de fabricantes (Samsung Internet antiguo, Mi Browser) si no están actualizados.

- **iOS (Apple):** Versión **16.4** o superior.
  - *Justificación:* Es la versión mínima requerida por Apple para soportar **Web Push Notifications** en PWAs instaladas en el Home Screen.
  - *Fallback:* En versiones anteriores (iOS 15+), la App funciona, pero el usuario **NO** recibirá notificaciones push cuando la app esté cerrada.

- **B. Hardware Mínimo:**

- **Cámara:** Trasera, Resolución 5MP+ con **Auto-Focus** (Cámaras de foco fijo no pueden leer QRs pequeños o IDs a distancia).
- **GPS:** Receptor GNSS nativo con precisión < 20 metros.
- **RAM:** 3GB Mínimo (Recomendado 4GB para renderizado fluido de mapas de calor).

- **C. UX de Incompatibilidad:** Si el sistema detecta un User-Agent inferior al soportado durante el Login:

- Muestra una alerta no bloqueante: "*Tu dispositivo es antiguo. Algunas funciones como el Mapa o las Notificaciones podrían fallar. Recomendamos usar Chrome actualizado.*"

- **RNF-7 Restricciones Operativas:** Control estricto de costos Twilio y cumplimiento Ley 1581.

- **Política de Exclusión de Menores (Voting Age Only):**

- **Restricción:** El sistema limita el registro exclusivamente a ciudadanos con **Cédula de Ciudadanía** (Mayores de 18 años). Se **prohibe** la captura de Tarjetas de Identidad (TI) o Registros Civiles.
- **Justificación Legal:** El mecanismo de aceptación de términos (RF-3.2) no está diseñado para el tratamiento de datos de menores (que requiere consentimiento cualificado de tutores), por lo que aceptar menores vulneraría la normativa de Habeas Data.
- **Justificación Operativa:** Garantizar que el 100% de la base de datos corresponda al **Potencial Electoral Activo** para evitar distorsiones en las proyecciones de votos del Día D.

- 

- **RNF-8: Segregación de Entornos y Modo Sandbox Financiero** El sistema debe operar en dos entornos estrictamente separados, controlados por variables de entorno (ENV\_VARS), para garantizar la seguridad financiera durante el desarrollo y QA.

- **A. Entorno de Producción (ENV=production):**

- **Billetera:** Dinero Real. Descuenta del saldo cargado por el Administrador.

- **SMS:** Utiliza credenciales vivas de Twilio. Los mensajes llegan a los votantes.
- **Visualización:** Interfaz limpia, sin marcas de agua.
- **Infraestructura (Always On):** Se configura la bandera --min-instances 1 en Cloud Run.

• *Objetivo:* Evitar la latencia de arranque en frío. El sistema siempre responde inmediatamente, incluso si es el primer usuario de la mañana.

#### • **B. Entorno de Staging (ENV=staging):**

##### • **Billetera Simulada (Mock Wallet):**

- El sistema inicia con un saldo ficticio de **\$5,000.00 USD (Fake)**.
- Las transacciones de gasto se registran en wallet\_transactions pero con una bandera isTest: true.
- **Feature:** Botón "Reset Saldo" visible en el Dashboard para que los testers puedan vaciar o llenar la billetera instantáneamente.

##### • **SMS Mocking (Twilio Magic Numbers):**

- El backend intercepta las llamadas a la API de Twilio.
- **No se envían SMS reales.**
- Se utilizan los *Test Credentials* de Twilio. Si se envía a un número mágico (ej: +15005550006), la API devuelve "Éxito" simulado. Si se envía a +15005550001, devuelve "Error", permitiendo probar el flujo de reembolso sin gastar dinero.

##### • **Indicador Visual de Seguridad:**

- Se muestra una **Barra Superior Naranja** persistente en toda la aplicación: "MODO PRUEBAS - STAGING (No se están enviando mensajes reales)". Esto evita que un coordinador confunda el entorno de pruebas con la campaña real.

##### • **Infraestructura (Scale-to-Zero):** Se configura min-instances: 0 (Default).

- *Ahorro*: El servicio se apaga totalmente cuando los desarrolladores no lo usan, reduciendo el costo a \$0 fuera de horario laboral.
  - *Efecto*: Se acepta una latencia inicial de 5-10 segundos en el primer acceso ("Cold Start").
- **RNF-9: Estrategia de Aseguramiento de Calidad (QA Automatizado)** Para garantizar la integridad de los datos y la estabilidad de los flujos críticos, se establecen los siguientes mandatos de cobertura:
    - **Pruebas Unitarias (Lógica de Negocio)**: \* **Cobertura**: 100% de cobertura de ramas (Branch Coverage) obligatoria para el **RF-3.5 (Matriz de Fusión de Datos)** y el **RF-1.9 (Prevención de Ciclos)**.
      - **Objetivo**: Garantizar matemáticas exactas en la resolución de conflictos sin depender de la base de datos.
    - **Pruebas E2E (Flujos Críticos)**:
      - **Herramienta**: Playwright.
      - **Escenarios Obligatorios**: 1. Registro completo de usuario nuevo (Flujo 1). 2. Escaneo de QR y redirección. 3. Simulación de "Modo Offline" (Network Interception) y posterior sincronización.

## 6. FLUJOS DE PROCESOS PRINCIPALES

### FLUJO 1: Registro con Redirección Dinámica (Smart QR)

1. Ciudadano escanea QR (M-001).
  2. Server Middleware registra hit y redirecciona a PWA.
  3. PWA carga formulario (Offline-Ready).
  4. Usuario completa datos personales y Ubicación de Vivienda (GPS/Manual).
  5. **Selección de Puesto (Opcional)**: El usuario escribe "Santa L..." en el campo de Puesto de Votación. El sistema filtra la lista local de voting\_places y muestra las coincidencias.
0. **Caso A (Éxito)**: El usuario selecciona una coincidencia oficial. Se guarda el ID.
  1. **Caso B (Fallo/Nuevo)**: No encuentra su puesto. Selecciona "No aparece". El sistema habilita un campo de texto, el usuario escribe el

nombre manualmente. El sistema guarda votingStationId: 'NON\_LISTED' y el nombre en texto plano.

6. Acepta Políticas (Legal + WhatsApp Opt-in).
7. El sistema guarda el registro en users e inserta atómicamente la membresía vinculada a la political\_campaign detectada en el paso 1. Sistema valida 'First-to-Sync'. Si hay GPS, asigna zona de inmediato. Si es Dirección Manual (Offline), se marca como 'Pendiente de Geo-Procesamiento' (Batch Nocturno) y se guarda el registro.
8. Cierre: Envío de enlace de invitación (si hubo consentimiento).

## FLUJO 1B: Vinculación Orgánica y Auto-Asignación (Sin QR)

1. **Registro Inicial:** Usuario se registra vía Web/App sin código de referido.
2. **Estado Neutro:** El sistema crea usuario con rol 'NORMAL'. El usuario ve una pantalla de "Inicio" genérica con lista de campañas públicas disponibles o buscador de candidatos.
3. **Intención:** El usuario selecciona una campaña y pulsa el botón **[SEGUIR / UNIRME]**.
4. **Validación de Datos:**
  - *Caso Falta Datos:* Sistema detecta address: null. Muestra modal: "Completa tu dirección". Usuario llena datos -> Sistema geocodifica.
  - *Caso Datos Completos:* Continúa al paso 5.
5. **Enrutamiento (Backend):**
  - Sistema consulta colección territorial\_zones de la campaña.
  - Calcula intersección de coordenadas del usuario vs. Polígonos.
6. **Vinculación (Write):**
  - Se crea objeto en memberships.
  - Campo recruitedBy = UID del Líder de la Zona encontrada (o Admin si no hay match).

7. **Activación:** La interfaz se recarga y muestra el Dashboard de Seguidor correspondiente a esa campaña (Ver RF-7.1).

**FLUJO 2: Generación y Distribución de QR** Multiplicador solicita código en PWA -> Server genera SVG -> Opciones: Descargar PNG o Copiar Enlace -> Distribución (WhatsApp/Impreso).

**FLUJO 3: Dashboard y Exportación Segura** Usuario solicita Exportar -> Sistema verifica Rol -> Si es Admin: Ofrece Modos (Master/Safe) -> Si es Coordinador: Bloquea y muestra error.

- **Paso Crítico (Advertencia de Trazabilidad):**

- Antes de iniciar la descarga, el sistema muestra un Modal Obligatorio:
- *Mensaje:* "Este archivo será marcado digitalmente con tu identidad (**[Nombre Usuario]**) y dirección IP. Eres legalmente responsable de su custodia bajo la Ley 1581. ¿Deseas proceder?"
- *Acción:* Al confirmar, se dispara la generación del archivo y la notificación de seguridad (Security Broadcast).

#### **FLUJO 4: Envío de Mensajes Segmentados**

1. **Configuración:** Crea Campaña de mensajería -> Selecciona Plantilla y Audiencia.
2. **Validación Externa (Nuevo):** El sistema consulta a Twilio/Meta el estado de la plantilla. Si es 'REJECTED', detiene el proceso.
3. **Pre-Flight Check:** Verifica Saldo vs Costo Estimado (RF-5.6).
4. **Aprobación:** El usuario confirma y la campaña de mensajería pasa a cola de envío.

#### **FLUJO 5: Derecho al Olvido (Anonimización Estructural)**

1. **Solicitud:** Usuario solicita baja desde perfil o vía legal.
2. **Validación:** Verificación de identidad estricta (OTP) para evitar sabotaje.
3. **Verificación de Dependencias:** El sistema identifica si el nodo tiene hijos.
4. **Ejecución de Script de Ofuscación:**

- Update en BD: Reemplazo de PII (Nombre, Teléfono) y liberación de Cédula (Hash temporal).

- Eliminación de Auth: Borrado del usuario en la tabla de autenticación.
5. **Resultado:** El usuario ya no puede hacer login. En el Dashboard del líder superior, este nodo aparece como "Usuario Eliminado" (gris), pero mantiene la conexión con los nietos de la red.
  6. **Auditoría:** Se genera log en audit\_logs registrando la acción de anonimización sin guardar los datos viejos.

## FLUJO 6: Recuperación de Acceso (Jerarquía de Soporte)

### A. Vía Autoservicio (Prioridad 1 - Email):

- Solicitud:** El usuario pulsa "¿Problemas para entrar?" en la pantalla de Login.
- Opción:** Selecciona "Enviar código a mi correo [c\*\*\*@gmail.com]".
- Entrega:** El sistema envía un token OTP al correo.
- Resolución:** El usuario ingresa el código y recupera el acceso inmediato. Costo Operativo: \$0.

### B. Vía Soporte Jerárquico (Prioridad 2 - Fallback):

- Reporte:** El usuario (ej: Multiplicador M-050) notifica a su Enlace/Coordinador: "*Perdí mi celular, mi nuevo número es 300-123...*".

#### 2. Validación de Identidad (Anti-Impersonation):

- **Acción:** El Coordinador solicita al usuario (M-050) una foto de su Cédula o la exhibición física de la misma.
- **Verificación:** El Coordinador compara el número del documento físico contra el documentId que figura en el Dashboard de la campaña para ese usuario.

0. *Si coincide:* Se procede con la solicitud.

1. *Si no coincide o no presenta documento:* Se deniega la solicitud por riesgo de robo de cuenta (Account Takeover).

#### 3. Gestión Administrativa:

- Coordinador envía ticket/solicitud al Admin con permisos de gestión.

- Admin accede a "Gestión de Usuarios" > Buscar "M-050".
- Selecciona opción: **[Actualizar Teléfono Seguro]**.

#### 4. Ejecución del Sistema:

- Input: Nuevo número (+57 300...).
- Process: El sistema actualiza el registro en Firestore y revoca las sesiones activas del token anterior.

#### 5. Re-ingreso:

- El usuario entra a la PWA e ingresa su **Nuevo Número**.
- Recibe OTP en el nuevo dispositivo.
- Al entrar, ve su Dashboard intacto (mismo historial, mismos seguidores).

### FLUJO 6B: Recuperación de Acceso por Pérdida de Dispositivo + Número

1. **Reporte:** El usuario (ej: Multiplicador M-050) notifica a su Enlace/Coordinador: "Perdí mi celular y cambié de número".
2. **Validación de Identidad (Human Firewall):**
  - **Acción:** El Coordinador solicita la Cédula Física.
  - **Verificación:** Compara documento físico vs. documentId en Dashboard.
  - **Nota:** Este paso es obligatorio. Sin él, no hay desbloqueo.
3. **Gestión Administrativa (Solicitud Out-of-Band):**
  - El Coordinador reporta la incidencia al **ADMIN** enviando la evidencia por el canal seguro externo (ej: "Solicito actualizar teléfono de M-050. Cédula verificada en sitio.").
  - El **ADMIN** accede manualmente al módulo "Gestión de Usuarios" en el Dashboard, busca al usuario y ejecuta la acción crítica.
4. **Ejecución del Sistema (Reset):** \* **Backend:** Desvincula el UID del número viejo (+57 300...) y lo vincula al nuevo número (+57 315...) en el Auth Provider. \* **Seguridad:** Revoca todas las sesiones activas.
5. **Re-ingreso (Rompiendo el Loop):**
  - El usuario entra a la PWA e ingresa su **NUEVO Número** (+57 315...).

- **Entrega de OTP:** El sistema envía el código al **NUEVO dispositivo** (que el usuario tiene en la mano).
- **Resultado:** Al validar, el sistema reconoce el UID histórico y restaura el acceso al Dashboard intacto.

## FLUJO 7: Reorganización Estratégica (Mass Reassignment)

1. **Acceso:** Admin accede al módulo "Gestión de Estructuras" > Pestaña "Reasignación".
2. **Configuración de Origen:** Busca y selecciona al Líder Actual (ej: Juan Pérez). El sistema carga sus 150 seguidores.
3. **Selección de Carga:** El Admin selecciona "Todos los seguidores" o marca casillas específicas manualmente.
4. **Configuración de Destino:** Busca y selecciona al Nuevo Líder (ej: María Gómez).
5. **Validación de Sistema (Pre-Flight):**
  - ¿El Destino está activo? (Sí)
  - ¿El Destino está dentro de la rama del Origen? (NO - Pasa validación).
6. **Ejecución:** El sistema actualiza el campo parentId y hierarchyPath de todos los nodos seleccionados.
7. **Auditoría:** Se genera un log en audit\_logs con actionPerformed: 'BULK\_MOVE', detallando quién autorizó y cuántos registros se movieron.

## FLUJO 8: Carga y Validación de Puestos (Admin)

1. **Fuente de Datos:** El Admin obtiene el listado (Excel/PDF) de la Registraduría.
2. **Ingreso:** El Admin accede a "Configuración > Puestos de Votación" y selecciona "Importar CSV" o "Crear Nuevo".
3. **Resolución Geográfica:**
  - El sistema toma la dirección del puesto (ej: "Calle 10 # 5-20").
  - Consulta a Google Geocoding API.

- Devuelve coordenada: Lat: 2.93, Lng: -75.28.
- Auditoría Visual:** El Admin ve el pin en el mapa. Si está correcto, pulsa [CONFIRMAR Y GUARDAR].
  - Disponibilidad:** El puesto queda inmediatamente disponible en el buscador del Formulario de Registro (Flujo 1).
- 

## 7. DISEÑO DE PANTALLAS (MOCKUPS FUNCIONALES)

### DIRECTRICES DE ESTILO (VISIBILIDAD EN CAMPO):

- **Tipografía:** Sans-serif (Inter/Roboto). Peso Bold para todos los encabezados y datos numéricos.
- **Color de Texto:** Prioridad al Negro Puro (#000000) sobre fondos Blancos (#FFFFFF). Evitar el modo oscuro automático en operaciones diurnas.
- **Delimitadores:** Usar bordes sólidos (border: 1px solid #000) en lugar de sombras suaves (shadow-md) para las tarjetas, asegurando que los límites sean visibles con brillo de pantalla bajo.

### PANTALLA 1: Formulario de Registro (PWA)

```
+=====+
| ÚNETE A NUESTRO MOVIMIENTO |
+=====+
| DATOS PERSONALES |
| [Nombre completo]] |
| [Cédula (ID)] [SPINNER ✕]] |
| [WhatsApp (+57)]] |
+-----+
| UBICACIÓN |
| (0) Usar mi GPS actual |
| () Ingresar manualmente |
| [Dirección / Barrio (Google Places)] |
+-----+
| MAPA (Visible solo Online) |
| [ⓘ] (Pin arrastrable) |
+-----+
```

|                                                                      |  |
|----------------------------------------------------------------------|--|
| LEGAL & PERMISOS                                                     |  |
| <input checked="" type="checkbox"/> Acepto Política Datos (Ley 1581) |  |
| <input type="checkbox"/> (Opcional) Recibir noticias Whats           |  |
| [ REGISTRARME ]                                                      |  |

[ELEMENTO FLOTANTE - SOLO iOS] (Tooltip en parte inferior apuntando a barra del navegador) "Instala la App: Toca Compartir [] y luego 'Agregar a Inicio'  
[+]" [X] Cerrar

### PANTALLA 1B: Formulario en Modo Fallback (Sin Mapa / Error API)

|                                                                      |                 |
|----------------------------------------------------------------------|-----------------|
| ÚNETE A NUESTRO MOVIMIENTO                                           |                 |
| DATOS PERSONALES                                                     |                 |
| [Nombre completo]                                                    |                 |
| [Cédula (ID)]                                                        | [SPINNER]       |
| [WhatsApp (+57)]                                                     |                 |
| UBICACIÓN                                                            |                 |
| [ICONO NUBE TACHADA] Modo Offline Activo                             |                 |
| No podemos cargar el mapa, pero tus datos se guardarán.              |                 |
| [Departamento (Select)]                                              | v (Huila)       |
| [Municipio (Select)]                                                 | v (Neiva)       |
| [Dirección Exacta]                                                   | (Cra 5 # 23-45) |
| LEGAL & PERMISOS                                                     |                 |
| <input checked="" type="checkbox"/> Acepto Política Datos (Ley 1581) |                 |
| <input type="checkbox"/> (Opcional) Recibir noticias Whats           |                 |
| [ REGISTRARME ]                                                      |                 |

[ELEMENTO FLOTANTE - SOLO iOS] (Tooltip en parte inferior apuntando a barra del navegador) "Instala la App: Toca Compartir [] y luego 'Agregar a Inicio'  
[+]" [X] Cerrar

### PANTALLA 1C: Modal de Bienvenida (Post-Registro)

|                              |  |
|------------------------------|--|
| [X] Cerrar                   |  |
| [ VIDEO PLAYER ]             |  |
| (Auto-play Muted)            |  |
| Candidato hablando a cámara: |  |

```
| "¡Hola [Nombre]! Bienvenido al equipo..." |
```

```
+-----+
| ¡YA ERES PARTE DEL CAMBIO!
```

```
Tu registro ha sido exitoso. Ahora puedes:
```

```
[(Icono WhatsApp) UNIRME AL CANAL DE NOTICIAS]
(Botón principal - Call to Action)
```

```
[Ir a mi Dashboard]
(Botón secundario)
```

## PANTALLA 2: Confirmación y QR Dinámico

```
+=====+
| ¡BIENVENIDO M-001!
```

```
+=====+
| #####
| ## ##
| ## SMART QR ##
| ## ##
| #####
+=====+
```

```
Enlace: connect.app/go/M-001
```

```
+=====+
| [Compartir WhatsApp] [Descargar PNG]
```

## PANTALLA 2B: Dashboard (Estado Vacío / Activación)

```
+=====+
| HOLA, [NOMBRE]
```

```
| Tu red está esperando. ¡Empecemos!
```

```
+=====+
| [QR GIGANTE M-001]
```

```
| "Muestra este código a tus amigos"
| [Compartir por WhatsApp]
```

```
+=====+
| ¿Prefieres hacerlo tú mismo?
```

```
| [(+) REGISTRAR MANUALMENTE A ALGUIEN]
```

```
+=====+
| (Los gráficos aparecerán aquí cuando
| tengas tu primer registro)
```

## PANTALLA 2C: Dashboard con Soft-Lock Activo (Vista Multiplicador)

```
+=====+
| [!] VALIDACIÓN DE CALIDAD EN CURSO
| Tu crecimiento ha sido muy rápido. Estamos validando tus
| últimos registros antes de liberar el acceso a herramientas
| avanzadas.
| [Puedes seguir registrando sin problemas]
+=====+
| HOLA, CARLOS (M-050)
| ...
+-----+
| | TU META: 120% (Sobrecumplida)
+-----+
| ACCIONES RÁPIDAS
| [(+) NUEVO REGISTRO] (Habilitado)
| [(v) EXPORTAR MI RED] (Deshabilitado - Color Gris)
+=====+
```

## PANTALLA 3: Dashboard Principal (Desktop - Vista Admin)

```
+=====+
| DASHBOARD CONNECT | Admin (Acceso Total) [Cerrar Sesión] |
+=====+
| PRESUPUESTO WHATSAPP (Control Manual)
| [#####.....] 42% Consumido
| Gastado: $4,200 | Disponible: $5,800 [+] RECARGAR (Solo Admin)
+-----+
| CRECIMIENTO REAL (Firestore Live)
| Total: 15,432 | Hoy: +127 | Líderes Activos: 340
+-----+
| ACCIONES ADMINISTRATIVAS
| [v] EXPORTAR EXCEL (Base Completa / Safe Mode)
| [>] NUEVA CAMPAÑA SMS
+=====+
```

## PANTALLA 3B: Dashboard Coordinador (Móvil / Adaptive)

```
+=====+
| Hola, Andrés! (Zona: Norte) |
+=====+
| TU META HOY: 78% Cumplida
| [#####...] Faltan 12 registros
+-----+
| MI EQUIPO (Tarjetas)
| +-----+
| | 1. Carlos Pérez
| | 234 votos | [Llamar] [WhatsApp]
| |
+=====+
```

|                               |                     |
|-------------------------------|---------------------|
| 2. María R.                   | [Llamar] [WhatsApp] |
| 198 votos                     |                     |
| [Casa] [Equipo] [Mapa] [Menu] |                     |

### PANTALLA 3C: Dashboard Enlace (Vista Táctica Municipal)

|                                                                                                                                 |
|---------------------------------------------------------------------------------------------------------------------------------|
| CONNECT   Enlace Municipal                                                                                                      |
| HOLA, JORGE (Enlace - Neiva)                                                                                                    |
| META MUNICIPIO: NEIVA (RF-7.2)<br>[     .....] 72%<br>5,400 / 7,500 Votantes                                                    |
| KIT DE DESPLIEGUE (RF-7.1.B.2)<br>(Acciones Rápidas de Campo)                                                                   |
| [QR] GENERAR CÓDIGO<br>Para nuevo líder                                                                                         |
| (v) CERTIFICAR LÍDER<br>Prueba de Vida (RF-3.11)                                                                                |
| TOP MOVERS (Tu Ranking Hoy)                                                                                                     |
| 1. Carlos P. (M-050) ..... +15 [Tel] [W]<br>2. Ana Maria (M-022) ..... +12 [Tel] [W]<br>3. Pedro J. (M-104) ..... +08 [Tel] [W] |
| ALERTAS DE GESTIÓN (Riesgo)<br>[!] 5 Líderes inactivos > 3 días<br>(Juan, Maria, Jose...)<br>[ REACTIVAR POR WHATSAPP ]         |
| [Inicio] [Mapa] [Mi Red] [Perfil]                                                                                               |

### PANTALLA 3D: Dashboard Seguidor (Vista Personal)

|                                                |
|------------------------------------------------|
| [MENU] [NOTIFICACIONES (3)]                    |
| (Campaign Switcher)                            |
| [ FOTO ] HOLA, CAMILA<br>(Seguidor Verificado) |

```

| [MIS CAMPAÑAS (2 Activas) >] |
+=====+
| TU PUESTO DE VOTACIÓN:
| Col. Santa Librada - Mesa 4
|
+-----+
| [MAPA ESTÁTICO - PIN VISIBLE] |
+-----+
| [EDITAR UBICACIÓN] |
+=====+
| ¿QUIERES APOYAR MÁS?
|
| Conviértete en Líder, obtén tu propio QR
| y ayúdanos a crecer.
|
| [¡QUIERO LIDERAR! (Icono Rayo)] | <- Trigger RF-1.4
+=====+
| NOTICIAS
| [Video: Mensaje del Candidato...] |
+=====+
| [Casa] [Mi Perfil] |
+=====+

```

#### PANTALLA 4: Mapa de Calor Híbrido

```

+=====+
| MAPA TERRITORIAL (@vis.gl/react-google-maps)
+=====+
| Modo Visualización:
| (x) Dónde Viven (Residencia) () Dónde Votan (Logística)
|
| [MAPA INTERACTIVO]
| (X) Alta densidad (Barrio Norte)
| (-) Media densidad
| () Baja (Oportunidad)
|
| *Nota: Si Google Maps falla, se carga Leaflet automáticamente
+=====+

```

#### PANTALLA 4B: Panel de Resolución de Disputas (Mapa)

```

+=====+
| (!) CONFLICTO TERRITORIAL DETECTADO
+=====+
| Hay una superposición de 450m2 entre:
| 1. Comuna 1 (Tu selección)
| 2. Comuna 2 (Vecino)
+-----+
| ¿CÓMO DESEAS RESOLVERLO?
|
| [CEDER] -> "Recortar mi zona, dejar el pedazo a Comuna 2"
+=====+

```

```
| [RECLAMAR] -> "Mantener mi zona, recortar a Comuna 2"
|
| [EDITAR MANUALMENTE]
+=====+
|
```

## PANTALLA 5: Gestión de Comunicaciones (Costos)

```
+=====+
| ENVIAR CAMPAÑA MASIVA
+=====+
| 1. Audiencia: [Seguidores Zona Norte (5,000)]
| 2. Plantilla: [Marketing_Evento_Cierre]
|
|-----|
| (!) ESTIMACIÓN DE COSTOS (Pre-Flight)
| Tarifa "Marketing": $0.04 USD / msg
| Destinatarios: 5,000
TOTAL A PAGAR: $200.00 USD
[(OK) APROBAR Y ENVIAR] [(X) CANCELAR]
+=====+
```

## PANTALLA 6: Feedback de Error Offline (Acción Bloqueada)

```
+=====+
| ENVIAR CAMPAÑA MASIVA
+=====+
| 1. Audiencia: [Zona Norte]
| 2. Costo: $200.00 USD
|
| [() APROBAR Y ENVIAR] <-- Click del usuario |
+=====+
|
| V (Disparador sin conexión)
|
+-----+
[!] ERROR DE CONEXIÓN
No es posible conectar con el servidor de
pagos.
Esta acción requiere internet estable para
evitar errores de facturación.
[REINTENTAR] [CANCELAR]
+-----+
(Fondo oscurecido / Backdrop Blur)
```

## PANTALLA 6B: Error Crítico de Almacenamiento (Device Full)

```
+=====+
| (!) MEMORIA DEL TELÉFONO LLENA |
+=====+
[ICONO DISCO ROJO]

No podemos guardar este registro porque tu celular no tiene
espacio disponible.

RIESGO DE PÉRDIDA DE DATOS:
No intente forzar el sistema.

ACCIÓN REQUERIDA:
1. Salga de la App (sin cerrar sesión).
2. Borre fotos o videos de su galería/WhatsApp.
3. Vuelva aquí y pulse "Reintentar".

[REINTENTAR GUARDADO] [CANCELAR REGISTRO]
+=====+
```

## PANTALLA 7: Consola de Resolución de Conflictos (Sync Audit)

```
+=====+
| CONFLICTO DE SINCRONIZACIÓN: CÉDULA 1.075.xxx.xxx |
+=====+
[REGISTRO ACTUAL (GANADOR)] [REGISTRO ENTRANTE (CONFLICTO)]
Recibido: 10:00 AM (Online) Capturado: 09:45 AM (Offline)
Por: Pedro (M-001) Por: Juan (M-002)

Nombre: Carlos Perez Nombre: Carlos A. Perez
Tel: 300 123 4567 Tel: 300 123 4567
Barrio: Las Granjas Barrio: Altico (Diferente!)

¿QUÉ ACCIÓN DESEA TOMAR?

[A] DESCARTAR ENTRANTE
"El registro original es correcto. Ignorar el nuevo."
-> Acción: Borra doc en 'sync_conflicts'. Notifica a Juan.

[B] ACEPTAR ENTRANTE (SOBRESCRIBIR)
"El dato nuevo es más reciente/preciso."
-> Acción: Update 'users', cambia 'recruitedBy' a Juan.

[C] FUSIÓN INTELIGENTE (MERGE)
"Mantener líder original, pero actualizar teléfono/barrio"
-> Acción: Update parcial de campos vacíos o distintos.
```

## PANTALLA 7B: Alerta de Conflicto (Lado del Usuario)

```
+=====+
| (!) YA ESTÁS REGISTRADO
+=====+
| Actualmente haces parte del equipo de:
| [FOTO AVATAR]
| Juan Pérez (Líder Zona Norte)
| Desde: 20 Nov 2025
+-----+
| Acabas de escanear el código de:
| María Gómez
+-----+
| ¿Qué deseas hacer?
|
| [MANTENERME CON JUAN] (Acción por defecto)
|
| [SOLICITAR CAMBIO A MARÍA] (Texto pequeño / Link)
| "Al solicitarlo, un coordinador revisará tu caso."
+=====+
```

## PANTALLA 8: Consola de Reasignación Masiva (Drag & Drop)

```
+=====+
| HERRAMIENTA DE REESTRUCTURACIÓN
+=====+
| [1. ORIGEN (Desde dónde)] | [2. DESTINO (Hacia dónde)] |
| Buscar: [Juan Perez (M-040)] | Buscar: [María Gomez (C-02)] |
|-----|
| [X] Seleccionar Todo (45 usuarios) | Zona: Norte
|-----| Nivel: Coordinador
| Lista de Usuarios a Mover:
| [X] Pedro A. (Seguidor)
| [X] Luis B. (Seguidor)
| [] Ana C. (Multiplicador) -> [Sub]
| [X] Carlos D. (Seguidor)
|
| [] >> MOVER SELECCIONADOS AL DESTINO >> []
+=====+
| RESUMEN DE LA OPERACIÓN:
| Se transferirán 3 usuarios de Juan a María.
| Juan conservará 42 usuarios.
|
| [CONFIRMAR CAMBIO] [CANCELAR]
+=====+
```

## PANTALLA 9: Constructor de Plantillas (WhatsApp Builder)

```
+=====+
| NUEVA PLANTILLA WHATSAPP |
+=====+
| Nombre Interno: [Invitación Cierre] |
| Categoría: (o) Marketing () Utilidad |
+-----+
| CONFIGURACIÓN VISUAL |
| [Cabecera] |
| Tipo: [Imagen (JPG/PNG) v] |
| [Subir Archivo...] (Vista previa cargada) |
| [Cuerpo del Mensaje] |
| "Hola {{1}}, te invitamos este {{2}} a la gran reunión..." |
| [+ Insertar Variable] |
| [Botones] |
| 1. [Visitar Web] -> https://micampaña.com |
+-----+
| VISTA PREVIA (Móvil) |
+-----+
| [IMG] |
| Hola Juan, te inv... |
| [Visitar Web] |
+-----+
+-----+
| [GUARDAR BORRADOR] [ENVIAR A APROBACIÓN (META)] |
+=====+
```

## PANTALLA 10: Consola de Configuración Global (System Config)

```
+=====+
| CONFIGURACIÓN DEL SISTEMA (MASTER SETTINGS) |
+=====+
| [PESTAÑA: FINANCIERO] [OPERACIÓN] [LEGAL] [SEGURIDAD] |
+-----+
| PARÁMETROS DE BILLETERA (Twilio/Wompi)
| Costo Unitario SMS (USD): [0.04] (Afecta cálculo de campañas)
| Límite de Gasto x Hora: [50.00] (Circuit Breaker RF-5.6) |
| [GUARDAR CAMBIOS FINANCIEROS] |
+-----+
| INTERRUPTORES DE EMERGENCIA (Feature Flags)
| [X] Permitir Nuevos Registros (RF-1.1) |
```

```

[] MODO EMERGENCIA (LITE VERSION - RF-3.10)
(!) Al activar: Se desactivan Mapas, Gráficos y Validaciones
lentas. Solo funciona el formulario básico. Usar en colapso.

[] MANTENIMIENTO (Cierra acceso a usuarios no-admin)

+-----+
| GESTIÓN DE CACHÉ
| [LIMPIAR CACHÉ DE METAS] [RE-INDEXAR BÚSQUEDA]
+=====+

```

## PANTALLA 11: Visor de Auditoría (Log Explorer)

```

+=====+
| AUDITORÍA DE SEGURIDAD Y TRAZABILIDAD
+=====+
| FILTROS:
| Rango: [Últimas 24h v] Actor: [Todos] Tipo: [BULK_MOVE v]
| Buscar por Cédula/ID Objetivo: [_____] [BUSCAR]
+-----+
| TIMESTAMP | ACTOR (Quién) | ACCIÓN | DETALLE / OBJETIVO |
+-----+
| 20 Nov 10:42 AM | admin_pedro | LOGIN | IP: 190.158.x.x (HQ) |
+-----+
| 20 Nov 10:15 AM | coord_maria | BULK_MOVE | Movió 45 usuarios
| | | | De: Juan -> A: Pedro
+-----+
| 20 Nov 09:30 AM | m_carlos | EXPORT_DATA | Descargó 'Zona Norte'
| | | (ALERT!) | (Masked Mode)
+-----+
| 20 Nov 08:10 AM | link_jorge | VIEW_PROFILE | Vio perfil de: Ana G.
| | | | (Silent Watcher log)
+-----+
| < Anterior [Página 1 de 50] Siguiente >
+=====+

```

---

## 8. ESPECIFICACIONES TÉCNICAS

### 8.1 Stack Tecnológico Recomendado

| Capa                        | Tecnología                  | Justificación                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Framework</b>            | <b>Next.js<br/>(Stable)</b> | <p><b>Política de Madurez:</b> Se utilizará la versión Estable más reciente disponible al inicio del desarrollo, descartando proyecciones específicas.</p> <p><b>Criterio de Seguridad:</b> Se exige estrictamente que la versión seleccionada tenga &gt; 1 mes de antigüedad en el mercado para garantizar que los parches críticos de lanzamiento hayan sido aplicados.</p> <p><b>Restricción:</b> Se prohíbe el uso de versiones <i>Canary</i>, <i>Beta</i> o <i>Release Candidates</i> en el entorno de Producción.</p> |
| <b>Lenguaje</b>             | <b>TypeScript</b>           | Tipado estático para robustez y mantenibilidad.                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Frontend</b>             | React + Tailwind CSS        | Mobile First, Shadcn/ui.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Visualización</b>        | <b>Recharts</b>             | <p><b>Optimización RNF-1:</b> Librería ligera basada en componentes React con soporte de <i>Tree-shaking</i>.</p> <p><b>Restricción:</b> Se prohíbe el uso de librerías de cómputo científico pesado (ej: Plotly.js, Highcharts full) para evitar inflar el tamaño del <i>bundle</i> principal en dispositivos móviles.</p>                                                                                                                                                                                                 |
| <b>Frontend<br/>(Lists)</b> | TanStack Virtual            | <b>Crucial para RNF-1.</b> Permite "Windowing" en listas largas (Infinite Scroll) sin degradar el rendimiento del DOM en móviles de gama baja.                                                                                                                                                                                                                                                                                                                                                                              |

| Capa                       | Tecnología                              | Justificación                                                                                                                                                                                                                                                                                                                                         |
|----------------------------|-----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Frontend<br>(Capabilities) | UAParser.js                             | Librería ligera para detectar OS y Browser en el cliente y mostrar las alertas del RNF-6 antes de que el usuario intente trabajar.                                                                                                                                                                                                                    |
| Base de Datos              | Firestore<br>(NoSQL)                    | Colecciones Planas. Persistencia offline.                                                                                                                                                                                                                                                                                                             |
| Storage                    | Google Cloud Storage                    | Fotos E-14. <b>Requiere:</b> Compresión cliente (WebP).                                                                                                                                                                                                                                                                                               |
| Auth                       | Auth.js v5<br>(Stable) o<br>NextAuth v4 | <p>Fijar versión exacta (Pinning) para evitar conflictos.</p> <p><b>Preferencia:</b> Auth.js v5 por menor tamaño de bundle y soporte nativo de Edge.</p> <p><b>Restricción (Safety Lock):</b> Solo se permite Auth.js v5 si está marcada como <i>General Availability (GA)</i>. De lo contrario, es obligatorio usar NextAuth v4 para producción.</p> |
| Nube / WAF                 | Google Cloud Platform + Cloud Armor     | <p>Cloud Run (Compute) y Cloud Armor (Seguridad WAF/DDoS). <b>Configuración Crítica:</b> Se establece min-instances: 1 en el servicio de Producción para mantener la memoria caliente, eliminando el 'Cold Start' de Next.js y garantizando respuestas &lt; 1s (RNF-1).</p>                                                                           |
| Secretos                   | Google Secret Manager                   | Almacenamiento encriptado de API Keys (Twilio, Maps). Evita <i>Hardcoded Credentials</i> y permite rotación segura.                                                                                                                                                                                                                                   |

| <b>Capa</b>          | <b>Tecnología</b>                              | <b>Justificación</b>                                                                                                                                                                                                                             |
|----------------------|------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Mensajería</b>    | Twilio API                                     | BSP oficial WhatsApp.                                                                                                                                                                                                                            |
| <b>Mapas (Prod)</b>  | Google Maps API                                | Places Autocomplete + SDK Mapas.                                                                                                                                                                                                                 |
| <b>Mapas (Dev)</b>   | <b>Leaflet / OSM</b>                           | Alternativa Open Source para reducir costos en desarrollo.                                                                                                                                                                                       |
| <b>Generación QR</b> | <b>node-qrcode</b>                             | Generación nativa interna (Costo \$0) en servidor.                                                                                                                                                                                               |
| <b>QA / Load</b>     | <b>Grafana k6</b>                              | Scripting JS para simulación de estrés (10x).                                                                                                                                                                                                    |
| <b>Async Queue</b>   | <b>Google Cloud Tasks</b>                      | Manejo de colas para geocodificación masiva (RF-6.7) y orquestación de envíos masivos de mensajería (RF-5.1). Permite "Rate Limiting" para controlar costos de APIs externas y evita Timeouts en Cloud Functions por procesos de larga duración. |
| <b>Uploads</b>       | <b>Background Fetch API + Firebase Storage</b> | Permite subidas resilientes (Chunked) que sobreviven al cierre de la app o bloqueo de pantalla (RF-3.9).                                                                                                                                         |
| <b>Unit Testing</b>  | <b>Jest o Vitest</b>                           | Validación estricta de la Matriz de Fusión (RF-3.5) y reglas de jerarquía.                                                                                                                                                                       |
| <b>E2E Testing</b>   | <b>Playwright</b>                              | Simulación de navegadores reales para validar flujos offline y Service Workers que Jest no puede probar.                                                                                                                                         |

| Capa                    | Tecnología                                          | Justificación                                                                                                                            |
|-------------------------|-----------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| Frontend<br>(Reporting) | CSS Print<br>Media<br>Queries                       | Generación de "Listados de Punteo" físicos sin costo de procesamiento servidor (PDF Serverless).                                         |
| Search<br>Engine        | Firestore<br>Native (Prefix<br>+ Security<br>Rules) | Búsqueda por rangos ( $>=$ , $<=$ ) con filtrado estricto por hierarchyPath. Se descarta Fuse.js (Cliente) por RAM y Algolia por Costos. |
| CI/CD                   | GitHub<br>Actions + WIF                             | Automatización de despliegue sin gestión de llaves JSON (Keyless), mitigando riesgos de fugas de credenciales en el repositorio.         |

## 9. FASES DE IMPLEMENTACIÓN

### FASE 1: MVP - Crecimiento y Estructura (4-6 semanas)

- Setup Next.js + Firestore (Flat Collections) + Tailwind.
- Configuración de Harness de Pruebas (Jest + Playwright).
- Registro PWA + Auth Passwordless + Offline Sync (First-to-Sync).
- Generación QR Nativa + Middleware Redirection.
- Zonificación básica y Mapas Leaflet.
- Definición de Schema "Día D" (Placeholders en BD sin implementación de UI).

### FASE 2: Expansion - Inteligencia y Comunicación (4-6 semanas)

- Mapas de Calor Híbridos (Google Maps en Prod). Integración Twilio (Opt-in filter + Wallet Manual).
- Dashboard Móvil (Adaptive UI) y Matriz RBAC.

### FASE 3: Advanced - Preparación Día D (6-8 semanas)

- Activación de UI para witness\_ids y Transporte.
- Módulo de Testigos y Logística.
- **Evidencia Digital (E-14):** Integración GCS + Compresión en cliente.
- **Pruebas de Estrés:** Escenarios k6 (50k usuarios).

## 10. CRITERIOS DE ACEPTACIÓN

1. **Offline:** Formulario guarda datos en Modo Avión y sincroniza al conectar (First-to-Sync).
2. **UI:** Componentes responden a móvil usando breakpoints de Tailwind.
3. **Legal:** Auditoría registra aceptación separada de Ley 1581 y WhatsApp.
4. **Seguridad:** Exportación bloqueada para no-admins. Admin exporta con máscaras DLP.
5. **Mapas:** Fallback automático a Leaflet si Google Maps falla. Fallback a Geocoding Server-side si no hay GPS.
6. **WAF:** Cloud Armor bloquea intentos de fuerza bruta.

## 11. ROADMAP Y TIMELINE

- **FINAL DE NOVIEMBRE 2025 (Semana 1):** Refinamiento v1.0. Freeze de Dependencias: Bloqueo de versiones en package.json (Pinning). Evaluación de estabilidad de la versión actual de Next.js (vs. LTS anterior). El Líder Técnico debe certificar la estabilidad de **Auth.js v5**. Si no cumple con los estándares de producción, se ejecuta el *rollback* a **NextAuth v4** antes de escribir la primera línea de código de negocio. Pruebas de compatibilidad entre el Framework seleccionado y **Auth.js v5** (o superior estable) para asegurar que el adaptador de Firestore funcione sin errores de hidratación.
- **DIC 2025 - ENE 2026 (Semanas 2-6):** Desarrollo MVP (Core DB Planas, PWA, QR, Cloud Run).
- **ENE - FEB 2026 (Semanas 7-12):** Módulos de Comunicación (Twilio Wallet), Mapas Avanzados y Smart Redirects.

- **FEB - MAR 2026 (Fase 3):** Módulo Día D, Integración GCS, Pruebas k6 y Lanzamiento.

## 12. MÉTRICAS DE ÉXITO

- **Adopción:** > 1000 nuevos registros diarios en mes 2.
- **Eficiencia QR:** > 80% de tasa de conversión.
- **Performance:** Dashboard móvil carga en < 2 segundos.
- **Presupuesto:** Desviación < 10% en costos de WhatsApp vs. Presupuesto Manual.
- **Disponibilidad:** Uptime 99.9% soportado por GCP y Cloud Armor.

## 13. ANEXOS: PLANTILLAS DE TEXTOS LEGALES (HABEAS DATA)

**Nota de Implementación:** Estos textos constituyen la configuración inicial para los campos de consentimiento definidos en el RF-3.2 y el RF-3.8. Deben ser validados por la asesoría jurídica de la campaña antes del despliegue en Producción.

### ANEXO A: Micro-Texto para Formulario de Registro (UI)

Texto corto a implementar junto al Checkbox del RF-3.2.

"Autorizo el tratamiento de mis datos personales, incluidos los sensibles (afiliación política) y la geolocalización (GPS), para la gestión de la campaña y el contacto vía WhatsApp según la [Política de Privacidad]."

### ANEXO B: Política de Tratamiento de Datos (Modal Completo)

Texto desplegable requerido para cumplir con el principio de finalidad de la Ley 1581, cubriendo los módulos técnicos del sistema:

#### AUTORIZACIÓN EXPRESA E INFORMADA

En cumplimiento del Régimen General de Protección de Datos Personales (Ley 1581 de 2012), autorizo al Candidato/Campaña ("El Responsable") y a sus proveedores tecnológicos ("Encargados") para tratar mis datos bajo las siguientes finalidades técnicas:

- **Gestión de Estructura Política:** Procesamiento de mi afiliación política (Dato Sensible) para la organización de equipos territoriales y asignación de roles de liderazgo.
- **Georreferenciación Operativa:** Captura y procesamiento de mis coordenadas geográficas (GPS) y dirección domiciliaria para la asignación de puestos de votación y zonificación territorial (Conforme al RF-6.1).
- **Canales de Mensajería:** Envío de información de campaña, noticias y alertas a través de servicios de mensajería instantánea (WhatsApp/SMS), entendiendo que puedo revocar este permiso específico en cualquier momento (Conforme al RF-5.1).
- **Auditoría y Seguridad:** Registro de mi dirección IP y huella digital del dispositivo para prevención de fraudes y duplicidad de identidad.
- **Retención Técnica en Respaldos (Permanencia Residual):** Entiendo y acepto que, en caso de solicitar la eliminación de mi cuenta, mis datos personales permanecerán almacenados de forma encriptada e inactiva ("Fuera de Uso") en las copias de seguridad del sistema por un periodo técnico máximo de **30 días**, con el único fin de garantizar la integridad ante desastres informáticos, tras lo cual serán destruidos definitivamente de forma automática.

**DERECHOS DEL TITULAR:** Declaro conocer mi derecho a consultar, actualizar, rectificar y solicitar la supresión de mis datos ("Derecho al Olvido"), procedimiento que podré ejercer a través de los canales oficiales de la campaña o mediante las herramientas de gestión de perfil dispuestas en la aplicación (Conforme al RF-8.3).