Trace-Vi FIUBA

Sistema de rastreo de contactos anonimizado

Olivia Fernandez, Ignacio Raik, Tomás Accini

Tutores: Mariano Beiró, Ignacio Alvarez Hamelin

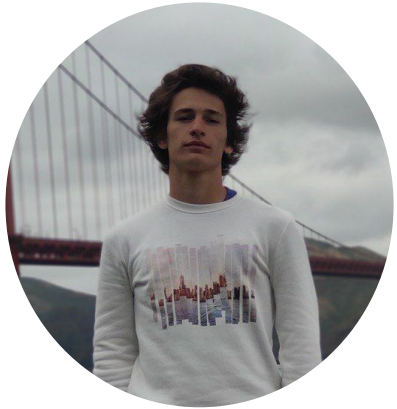
Agenda

- Quienes somos
- Problemática y contexto
- Motivación
- Nuestra solución
- Demo
- Evaluación de la solución

Nosotros

Olivia Fernandez
Ingeniería Informática

Ignacio Raik
Ingeniería Informática



Tomás Accini
Lic. en Análisis de Sistemas

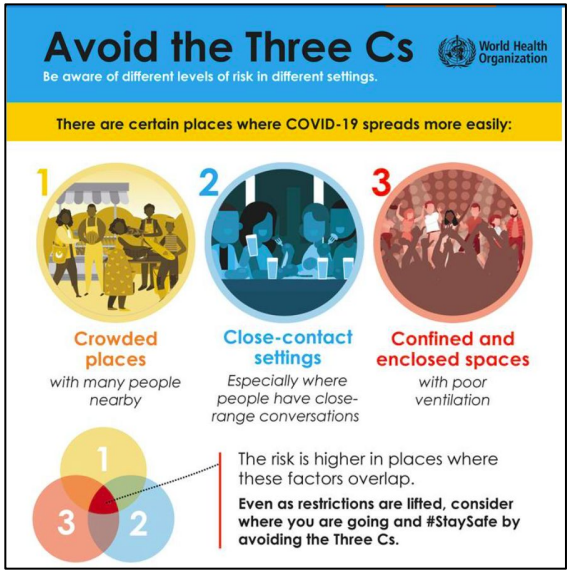
Problemática

Problemática

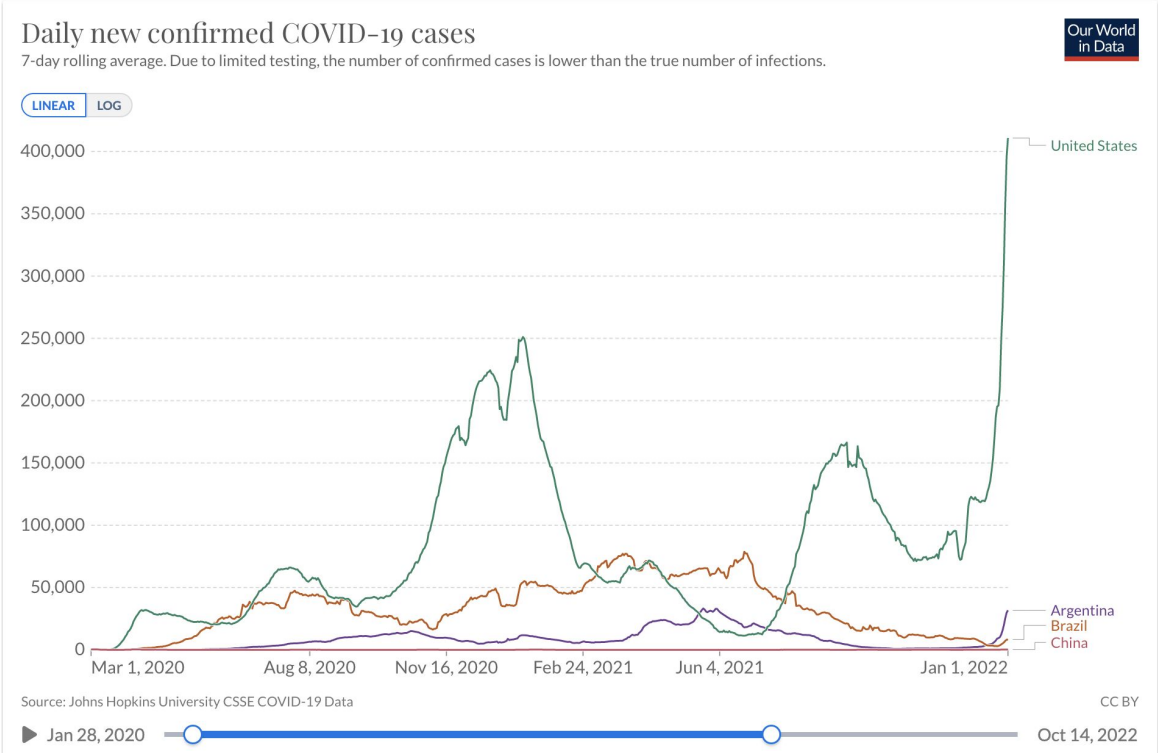
En 2020 surge la pandemia del COVID-19 que conmocionó al mundo. Ante lo inédito de la situación, se adoptaron distintas medidas para tratar de paliar la propagación de la enfermedad.

Problemática - Medidas adoptadas

- Cuarentena estricta
- Movilidad limitada
  - Grupos esenciales pueden circular
  - El resto de la sociedad solo puede salir a realizar actividades puntuales
- Desarrollo y aplicación de vacunas



Problemática - Enfoques adoptados

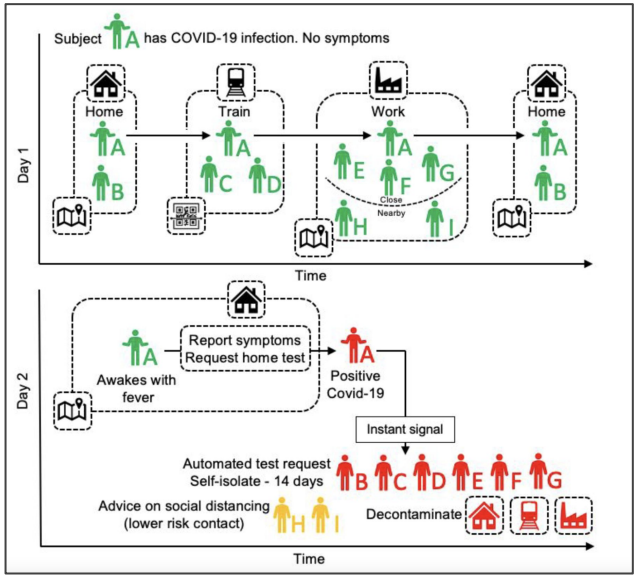


Motivación

Antecedentes

Alipay Health Code (China 🇨🇳) [Feb 2020]

- Monitoreo total
  - Sistema green-orange-red
- Movilidad controlada
- Epidemia mitigada



† https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html
† https://github.com/BDI-pathogens/covid-19_instant_tracing/blob/master/Policy%20forum%20-%20COVID-19%20containment%20by%20herd%20protection.pdf

Motivación [Otoño 2020]

- Construir sistema de rastreo con anonimización
  - Evitar rechazo por parte de Occidente
- Visibilizar el riesgo de contagio
- Extensibles a diferentes enfermedades
- Incorporar contexto del contacto
  - Espacios, vacunas, reincidencia
- Interés por parte del Hospital de Clínicas
- Sumar al aporte de FIUBA en el contexto de pandemia

Acciones de la FIUBA en el contexto de la pandemia

- **Predicción de contagios**: algoritmo para predecir contagios en base al movimiento de los individuos.
- **TermoCOVID19**: relevar en tiempo real síntomas de los habitantes del país de forma anónima.
- **FarmaCov test**: primer test rápido serológico de desarrollo nacional que detecta anticuerpos de COVID-19 en 5 minutos.
- **Ventilación dual:** desarrollo dispositivo bioseguro que permite el uso de un solo respirador para dos pacientes.

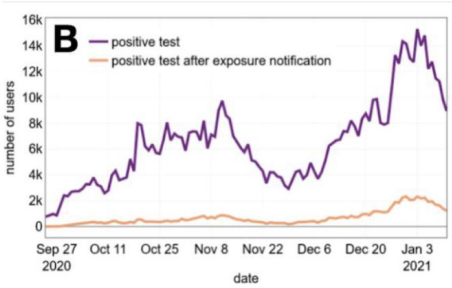
Relación con el hospital de clínicas

- Interés en implementar nuestra solución
- Feedback sobre el diseño de las aplicaciones y QRs
- Nuevos requerimientos:
  - Más características de los espacios (n95 obligatorio, ventilación)
  - Escanear QR de salida
  - Tiempo esperado de visita

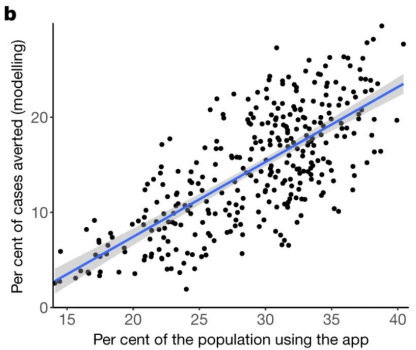
Motivación - Casos similares exitosos

NHS COVID-19 (UK 🇬🇧) [Sept 2020]

- Monitoreo anonimizado
- Sugerencias de aislamiento
- Reducción de curva de contagios



SAR among individuals notified by the app			6%
Cases and deaths averted in phases 1 and 2:		**Cases**	**Deaths**
From modelling of digital tracing		284,000 (108,000–450,000)	4,200 (1,600–6,600)
From matched-neighbours regression		594,000 (317,000–914,000)	8,700 (4,700–13,500)
	Per cent reduction in cases for every percentage point increase in app use		
Main analysis	**Phase 1**	**Phase 2**	**Overall**
Modelling	0.33 (0.13–0.49)	0.93 (0.46–1.24)	0.79 (0.37–1.10)
Matched-neighbours regression	1.09 (0.04–2.14) (bootstrap: 0.15–2.16)	2.66 (1.75–3.56) (bootstrap: 0.80–4.71)	2.26 (1.50–3.00) (bootstrap: 1.60–3.19)
Secondary analyses	**Phase 1**	**Phase 2**	**Overall**
Stratified linear regression in clusters[a]	−1.05 (−2.08 to −0.04)	3.34 (2.53–4.14)	2.76 (2.16–3.35)
Matched pairs regression[a]	5.08 (1.77–8.40)	3.89 (1.05–6.74)	4.39 (1.70–7.08)
Matched-pairs regression adjusted for local efficiency of manual contact tracing[a]	4.49 (0.21–8.77)	3.11 (−0.14–6.35)	3.67 (0.31–7.02)



† https://www.wehealth.org/blog/what-does-the-success-of-the-nhs-app-tell-us-about-other-en-apps
† https://www.nature.com/articles/s41586-021-03606-z

Técnicas y protocolos - (1) General

Arquitecturas:

- Centralizadas: back-end recolecta toda la información, identifica los usuarios con riesgo y los reporta.
- Descentralizadas: back-end server solo recibe y alerta sobre nuevos infectados; dispositivos interactúan entre sí y calculan sus propios riesgos de contagio.

Técnicas para compartir la información:

- Beacons Bluetooth device-to-device
- Share location history
- Reporte de visitas a establecimientos. Tecnologías:
  - Wifi
  - QR scans
  - Balizas Bluetooth

Técnicas y protocolos - (2) PEPP-PT

Características:

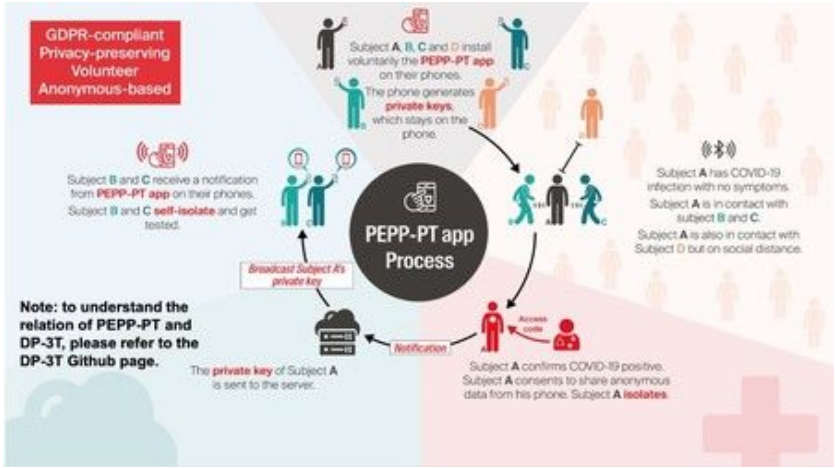
- Centralizado
- Contactos:
  - Bluetooth beacons para registrar contactos
  - Contactos se reportan al back-end de forma anonimizada
  - Al querer registrar un infectado, se tramita un código de autorización y se comparten en batch via HTTPs los beacons de los usuarios con los que se tuvo contacto
- Privacidad: Usuarios con seudónimos
- Autenticación: Registración de cuentas

Ventajas:

- Dispositivos no realizan procesamiento
- No requiere acción por parte del usuario
- Verificaciones en el servidor son más fiables

Desventajas:

- Consumo de batería (Bluetooth)
- Requiere que el Bluetooth esté siempre conectado
- Uso de servidor central



Técnicas y protocolos - (3) DP-3T

Características:

- Descentralizado
- Contactos:
  - Bluetooth beacons para registrar contactos
  - Contactos se intercambian entre dispositivos
  - Al querer reportarse infectado, se gestiona y autoriza un reporte para cargar espaciadamente los beacons a una cartelera virtual
- Privacidad: Ephemeridal IDs
- Autenticación: -

Ventajas:

- Al no requerir de servers third-party, ofrece mayores garantías de privacidad
- No requiere acción por parte del usuario

Desventajas:

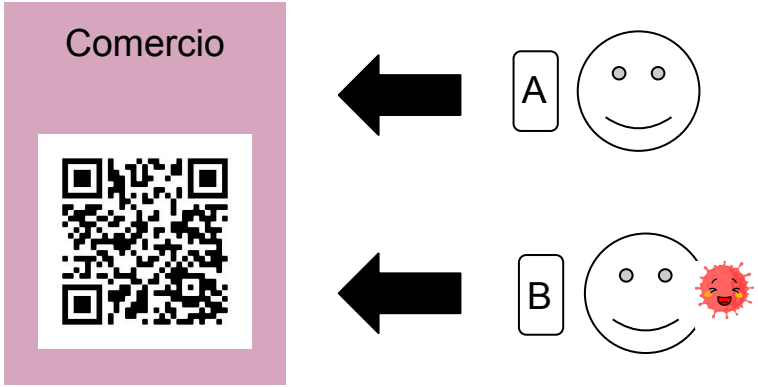
- Basto uso de recursos del dispositivo (batería, CPU)
- Requiere que el Bluetooth esté siempre conectado
- Vulnerable a múltiples tipos de ataques informáticos (a servers y usuarios)

Nuestra solución

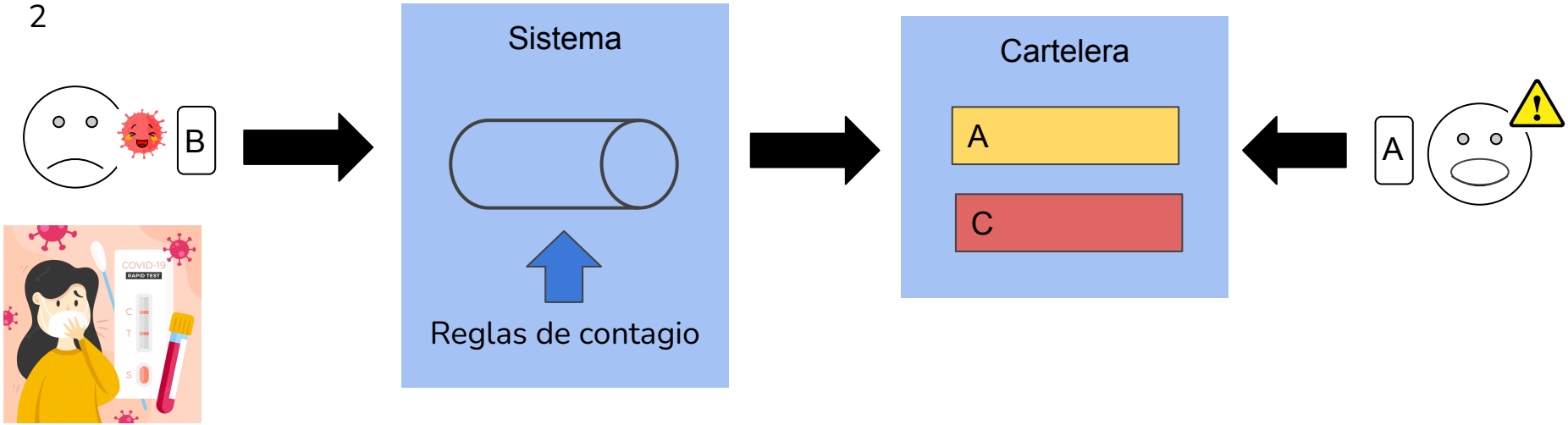
Objetivo

- Preservación de privacidad
- Resistente a uso ilegítimo
- Escalabilidad
- Información contextual para el cálculo de riesgos
- Reglas de contagio dinámicas
- Poco consumo de recursos de los dispositivos
- Sin Bluetooth
- UX simple

1

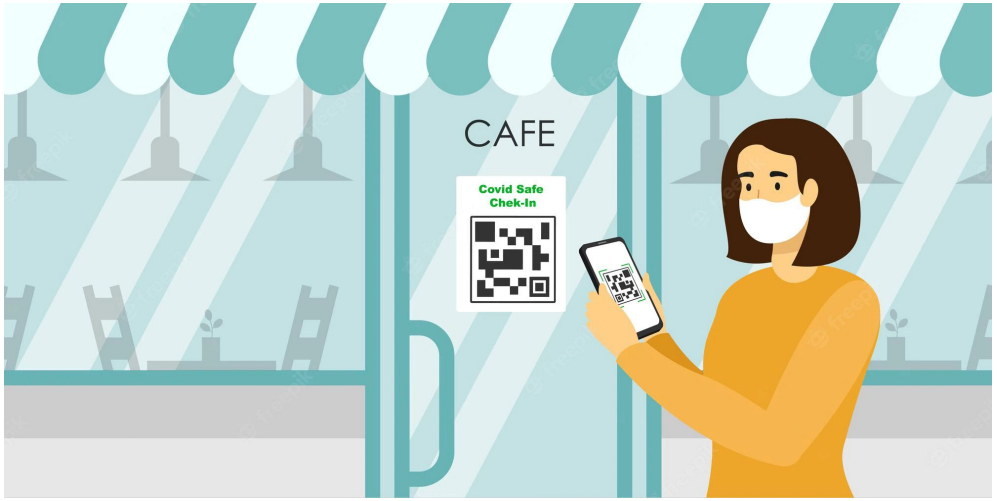

Comercio
A
B

2

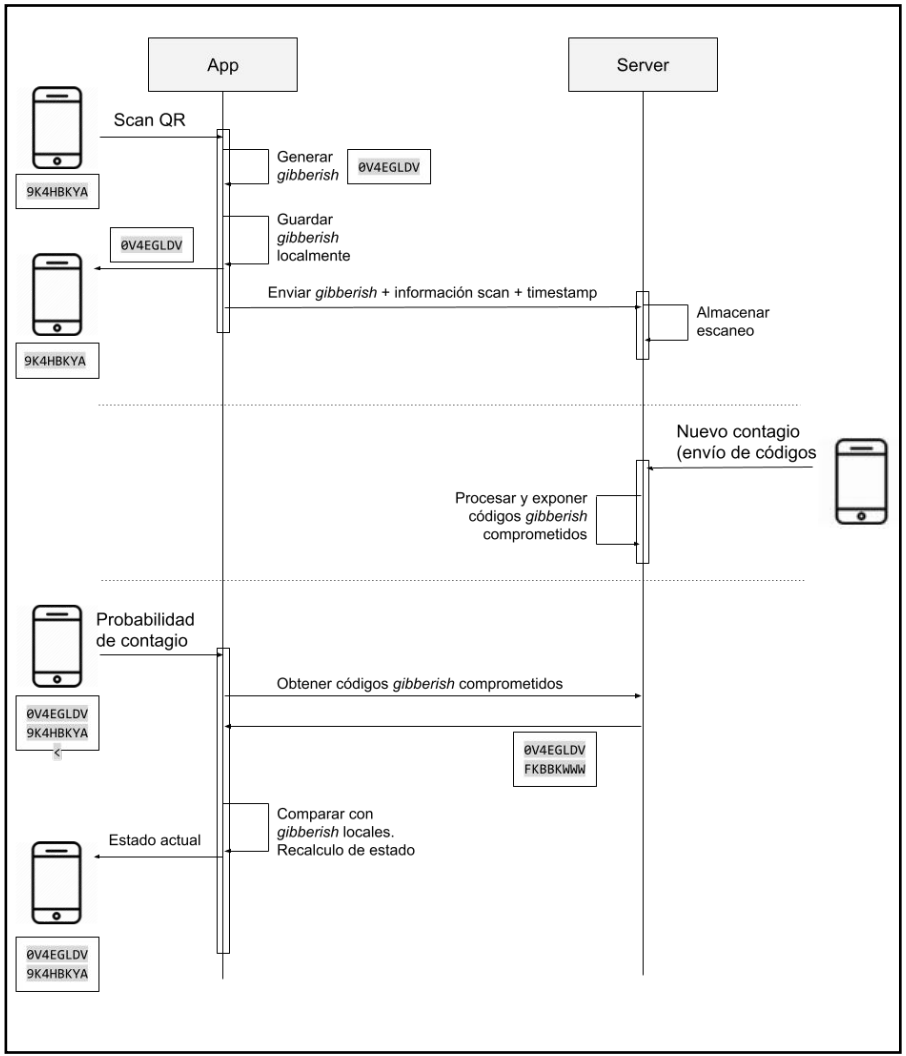

B
Sistema
Reglas de contagio
Cartelera
A
C
A
COVID-19
RAPID TEST

Usuarios

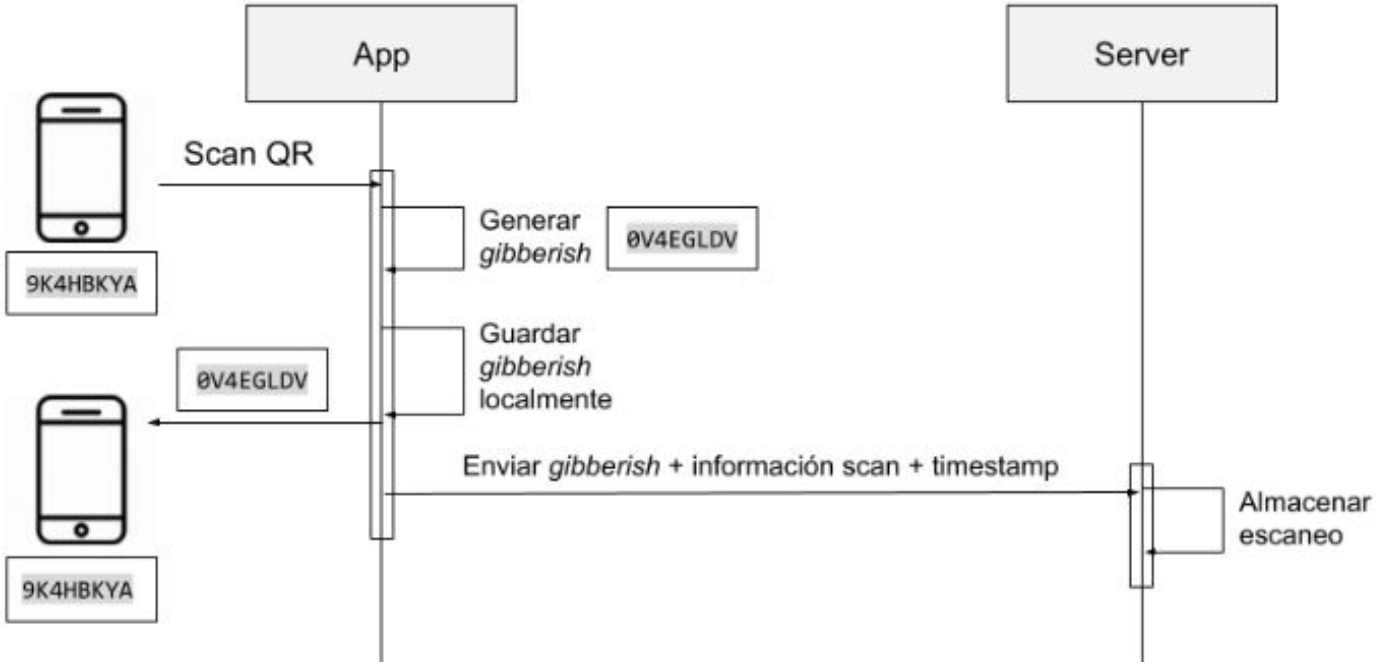
- Usuarios de las apps
- Administradores
- Gestores de establecimientos



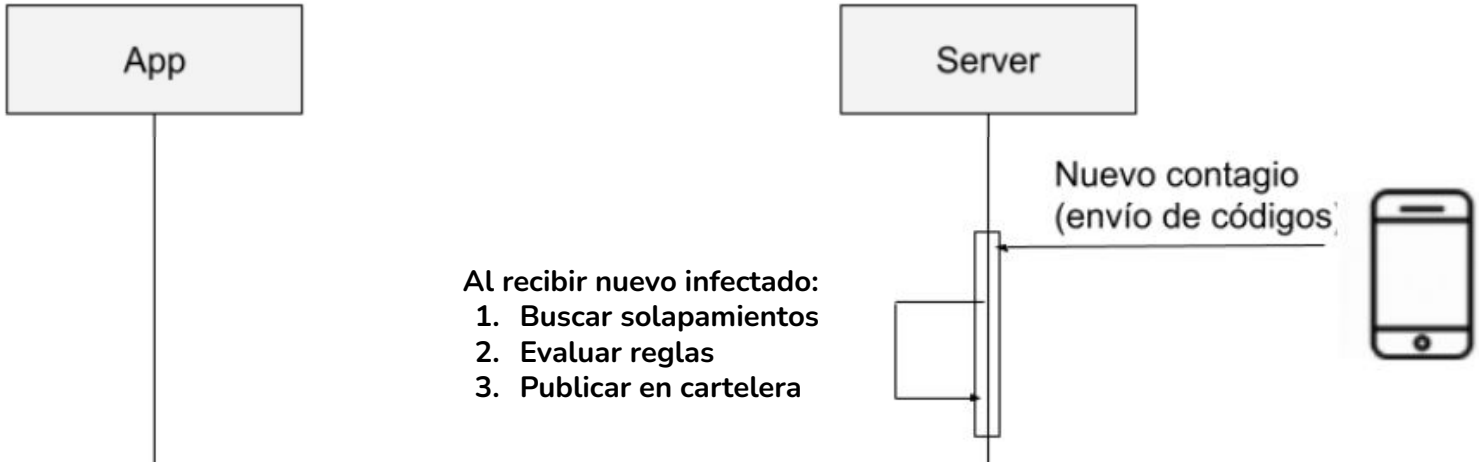
Detalles de la solución - Secuencia



Detalles de la solución - Escaneo



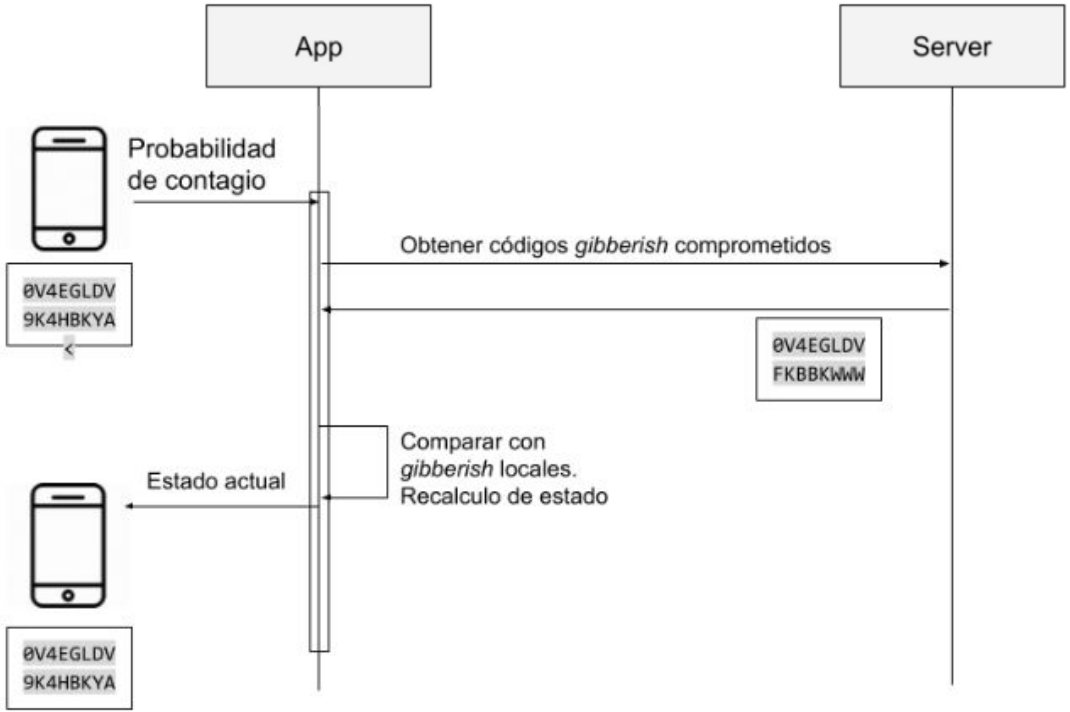
Detalles de la solución - Contagio



Al recibir nuevo infectado:

1. **Buscar solapamientos**
2. **Evaluar reglas**
3. **Publicar en cartelera**

Detalles de la solución - Actualizar riesgo



Detalles de la solución - Anonimización

- Visita compuesta por:

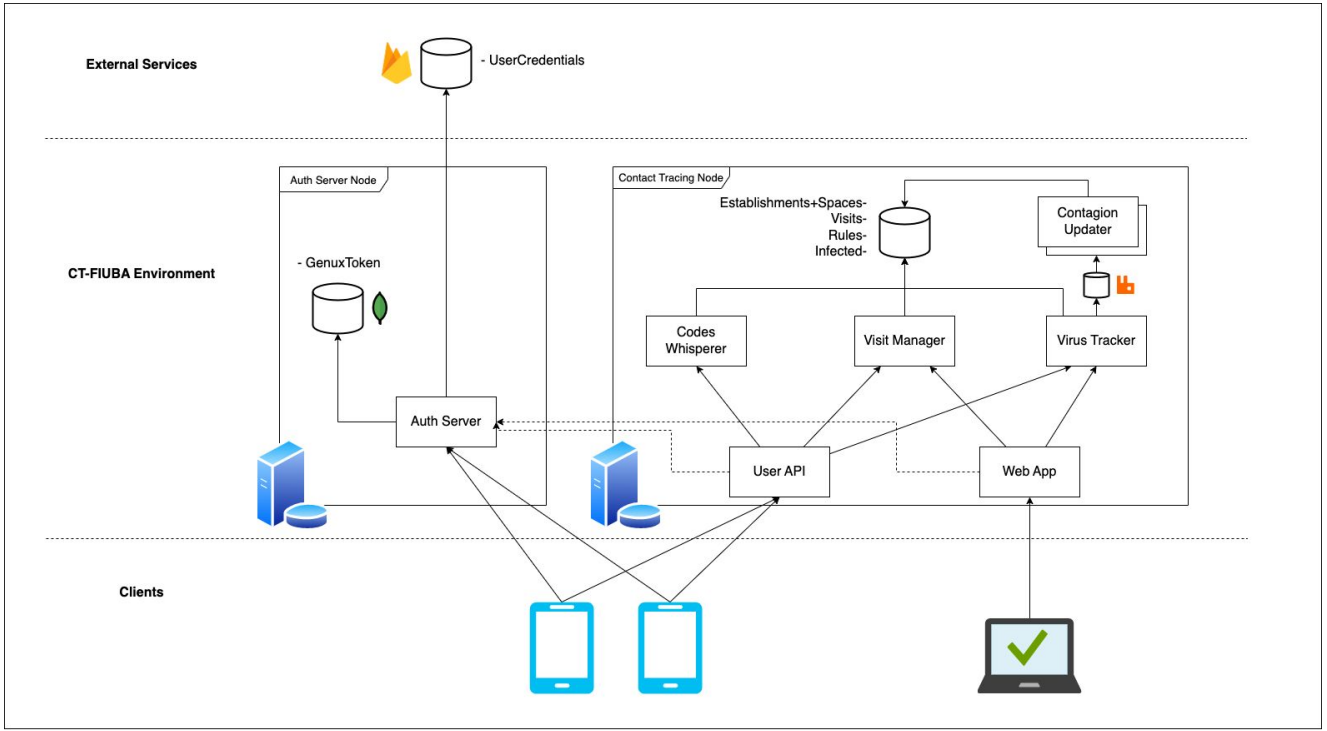
  (info espacio, timestamp, código generado, info contextual)

- Código generado:
  - Para cada visita se genera un código nuevo.
  - No es posible identificar al usuario.
  - No es posible determinar si dos códigos fueron generados por el mismo usuario.
  - Sólo la persona que lo generó puede saber si es suyo.

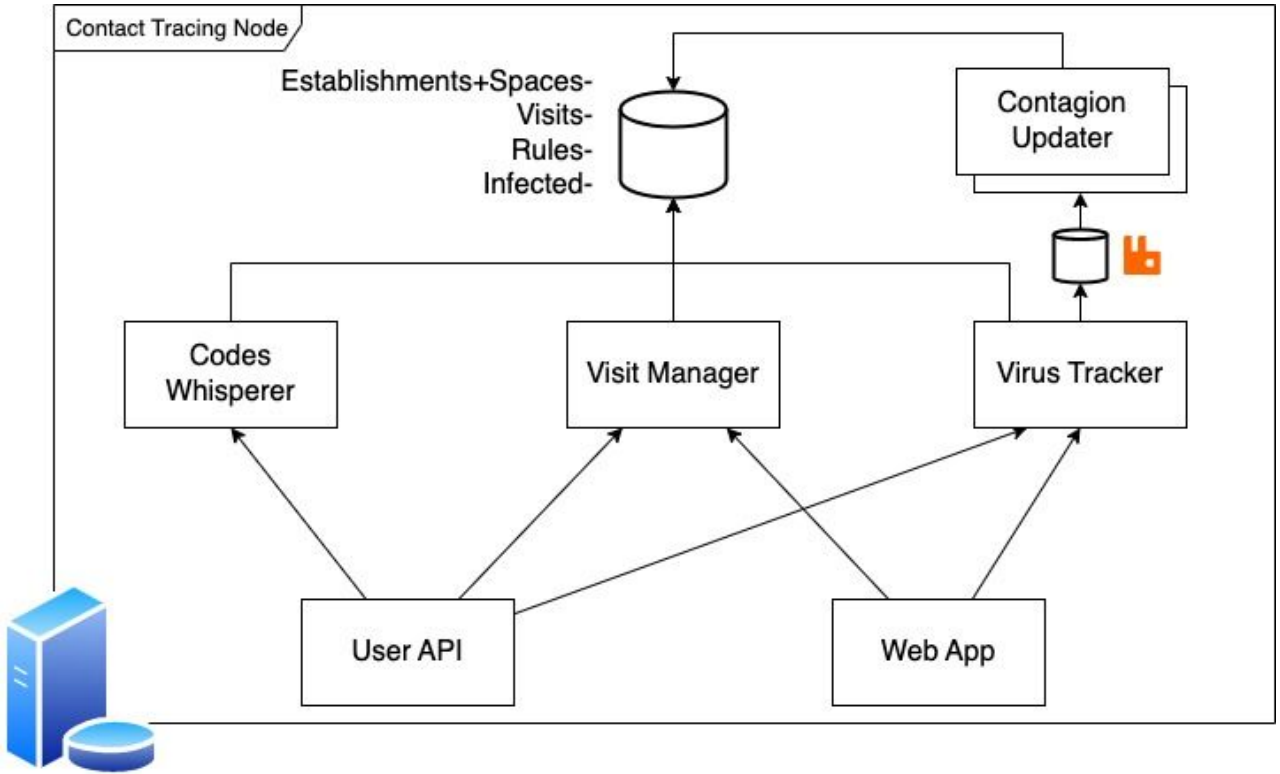
Detalles de la solución - Autenticación

- Necesario para evitar cargas ilegítimas sobre el sistema
- No puede ser autenticación clásica
  - Token no puede contener información del usuario
  - Token no puede ser utilizado para registrar infinitas visitas
- Solución → *Genux token*
  - Token opaco, de 1 sólo uso
  - Generado y validado por el Auth server
  - Negociado por la app por cada visita

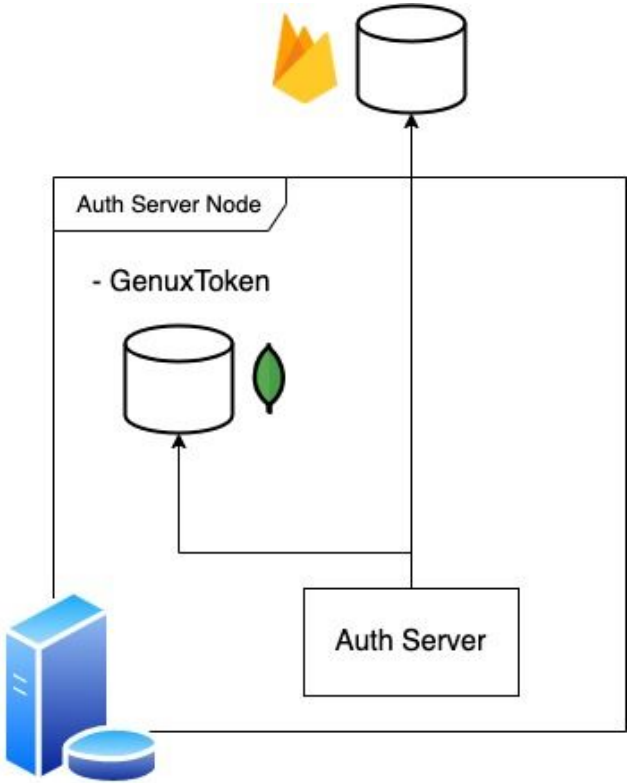
Detalles de la solución - Arquitectura



Detalles de la solución - Arquitectura

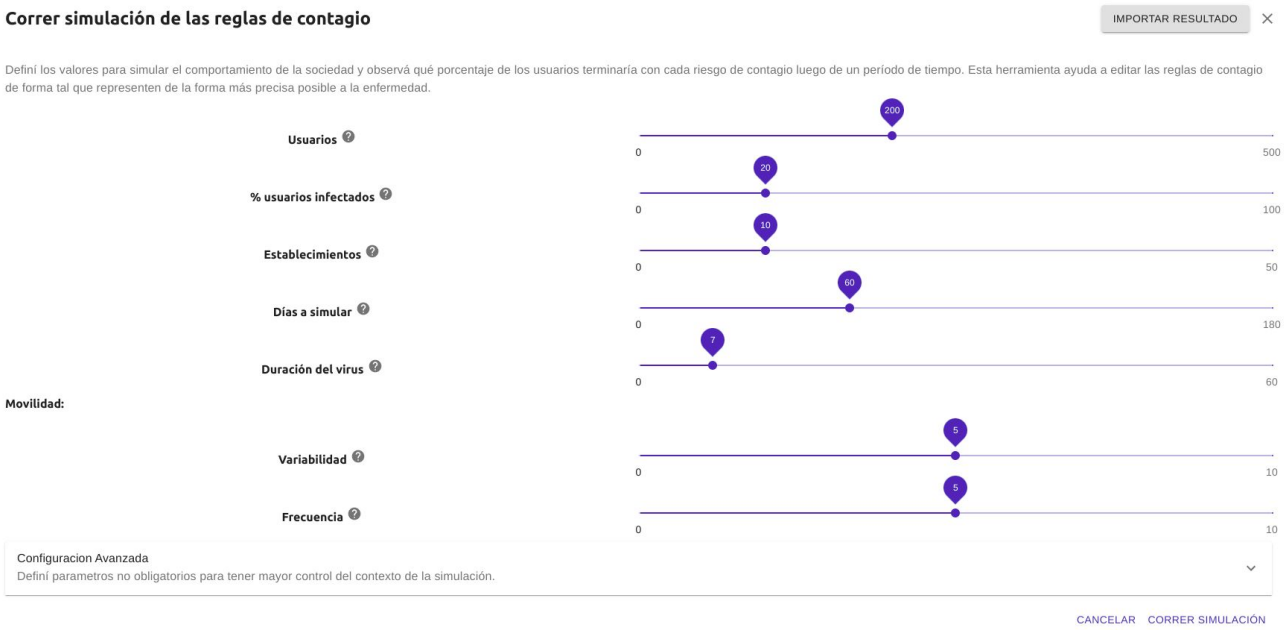


Detalles de la solución - Arquitectura



Detalles de la solución - Simulación (1)

- Manera de testear el comportamiento de las reglas
- Población uniforme



Detalles de la solución - Simulación (2)

- Output:

Estado final

Usuarios infectados: **0**

Usuarios con riesgo alto: **0**

Usuarios con riesgo medio: **0**

Usuarios con riesgo bajo: **200**

DESCARGAR RESULTADO

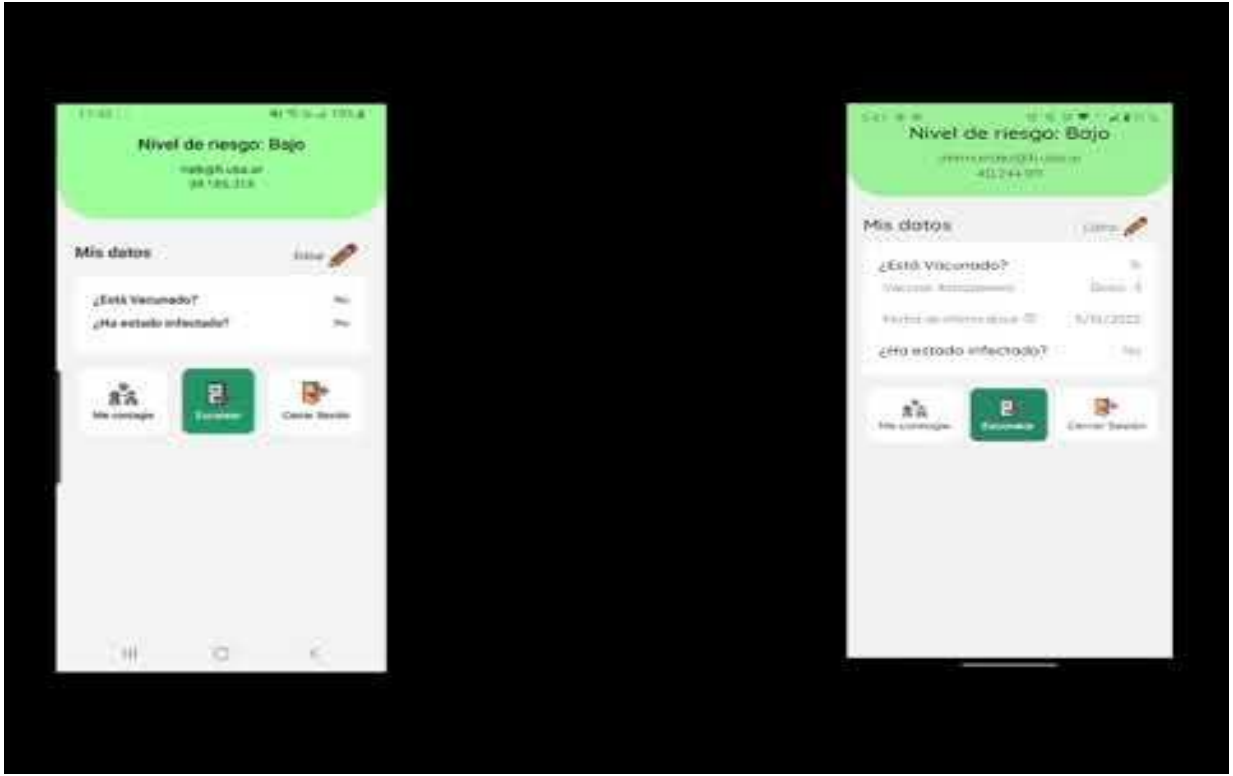
Demo!

Demo

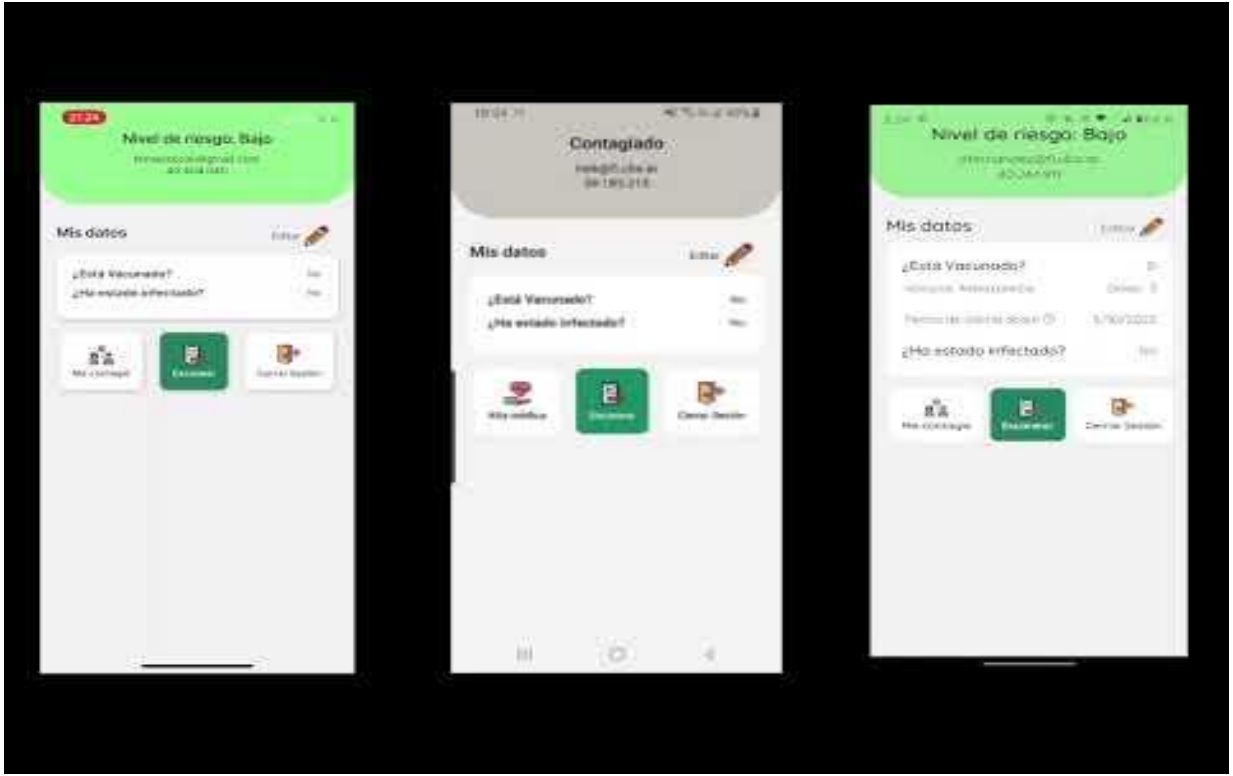
- Uso de la web interface
  - Vista administrador
  - Vista gestor de establecimientos
- Uso de la app mobile

Teniendo la app de Expo instalada:

Demo - Corridas de escenarios (1)



Demo - Corridas de escenarios (2)



Evaluación

Evaluación de la solución

- Análisis RQ3 →
- Pruebas :
  - Unitarias
  - End to end
  - Manuales
  - Performance
- Portabilidad:
  - iOS y Android
  - Despliegue local y remoto

Architecture Type		**Centralized**
User Privacy Exposure	*Generic User*	**Nivel 3**
	At-Risk User	**Nivel 3**
	Diagnosed User	**Nivel 3**
Threats	*Linkage Attack by Server*	**Riesgo improbable**
	Linkage Attack by Users	**Sin riesgo**
	False-Positive Claims	**Riesgo probable**
	Relay Attack	**Sin riesgo**

† https://arxiv.org/pdf/2006.10933/

Evaluación de la solución

- Análisis RQ3
- Pruebas :
  - Unitarias → ✅ 107 tests
  - End to end → ✅ 31 scenarios (https://github.com/ct-fiuba/e2e-test-suite)
  - Manuales
  - Performance → 100 establecimientos, 10000 usuarios, 55k visitas (~500 requests x seg)
- Portabilidad:
  - iOS y Android
  - Despliegue local y remoto

† https://arxiv.org/pdf/2006.10933/

Evaluación de la solución

- Análisis RQ3
- Pruebas :
  - Unitarias
  - End to end
  - Manuales
  - Performance
- Portabilidad:
  - iOS y Android ✅
  - Despliegue local y remoto ✅

† https://arxiv.org/pdf/2006.10933/

Evaluación de la solución

- Análisis RQ3
- Pruebas :
  - Unitarias
  - End to end
  - Manuales
  - Performance
- Portabilidad:
  - iOS y Android
  - Despliegue local y remoto

Architecture Type	✅	**Centralized**
User Privacy Exposure	*Generic User*	**Nivel 3**
	At-Risk User	**Nivel 3**
	✅ *[illegible]anced User*	**Nivel 3**
Threats	*Linkage Attack by Server*	**Riesgo improbable**
	✅ *Linkage Attack by Users*	**Sin riesgo**
	✅ *[illegible]e-Positive Claims*	**Riesgo probable**
	Relay Attack	**Sin riesgo**

✅ 107 tests

✅ 31 scenarios

✅ 100 establecimientos
10000 usuarios
55k visitas (~500 requests x seg)

† https://arxiv.org/pdf/2006.10933/

PEPP-PT vs DP-3T vs Nuestra solución

Características		**PEPP-PT**	**DP-3T**	**Trace-vi**
Tipo de arquitectura	Registro de contactos	Centralizado	Descentralizado	Centralizado
	Consulta de riesgo	Centralizado	Descentralizado	Descentralizado
Interaccion de Usuario		No requiere acción del usuario (bt)	No requiere acción del usuario (bt)	Requiere acción del usuario (QR scan)
Tecnología		Bluetooth siempre activado	Bluetooth siempre activado	No usa Bluetooth
Información contextual		No incluye	No incluye	Incluye

¡Gracias!

github.com/ct-fiuba