Tecnológico de Monterrey

TC2007B.401

Integración de seguridad informática en redes y sistemas de software

(Gpo 401)

“Etapa 3: Desarrollo”

Integrantes:

Juan Carlos Ferrer Echeverría	A01734794
Maximiliano Romero Budib	A01732008
Oscar Sebastián Martínez Sánchez	A01379654
Maximiliano Soberano Ramón	A01733902
Diego Gael Villaverde Nieves	A01275147

Mtra. Claudia Verónica Pérez Lezama

Mtra. Rosa Guadalupe Paredes Juárez

Mtro. Alam Lastra Mosqueda

Mtro. Fabio Galo Domínguez

18 de Octubre de 2022

URL del repositorio de software con el código del servidor, código del cliente

Carpeta de Drive que contiene ambas versiones de la aplicación:
https://drive.google.com/file/d/13Guno8uvAb-Mm90efkb8_P4UZNO5gl9i/view?usp=sharing

Configuración de la infraestructura

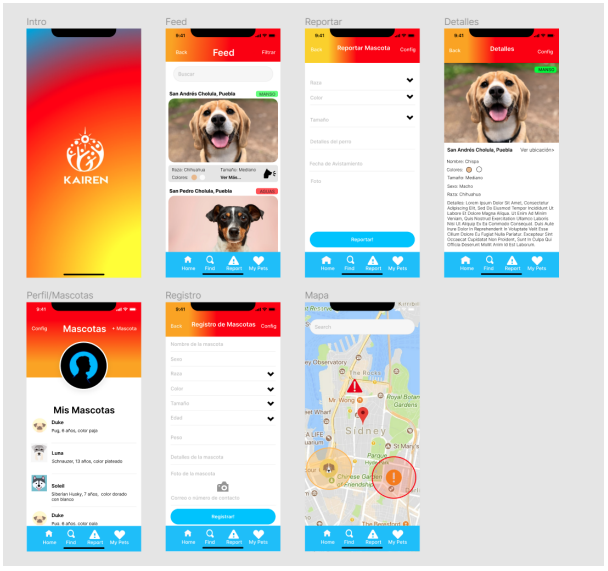
Para la configuración utilizamos Firebase de Google, para realizar nuestro servidor y base datos gratuitos (se paga cuando sobrepasa un límite de datos). Para poder hacer uso de esta herramienta entramos al siguiente enlace:

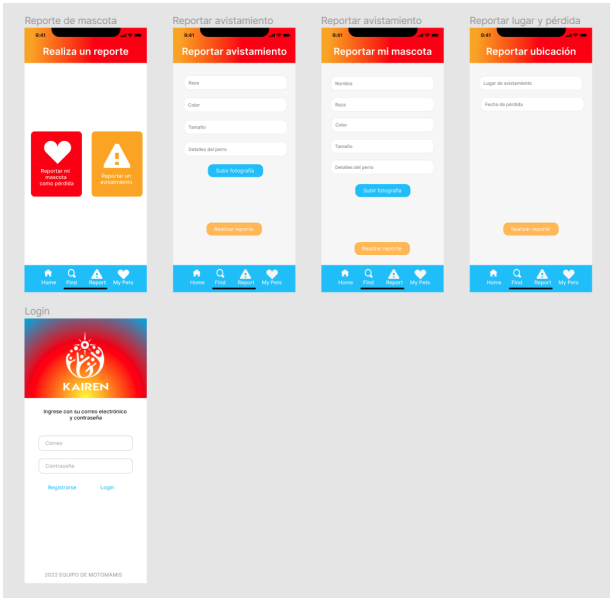
https://firebase.google.com/?hl=es-419&gclid=CjwKCAjw-rOaBhA9EiwAUkLV4hqGBafKjHB3gBqLYm4tkb75wM-B5lxzAjaKoRwYg8hnZinZUcTupRoCmawQAvD_BwE&gclsrc=aw.ds

Documentación con el cliente

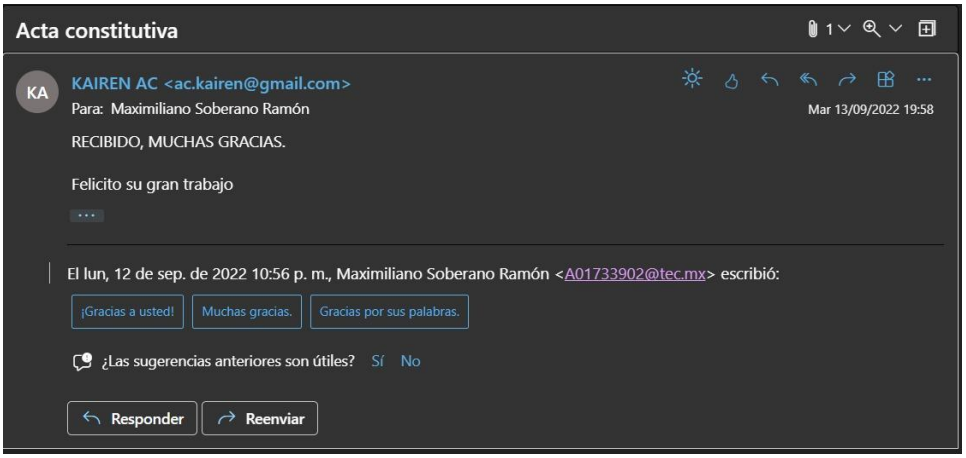
Nuestro primer acercamiento con el cliente fue durante las primeras semanas de clases en donde Kairen platicó con nosotros y nos presentó su idea sobre la aplicación que quiere desarrollar.

Posteriormente a esto comenzamos a trabajar en nuestro mockup de la aplicación para poder presentarlo al socio formador. Cuando finalmente llegó el día de la presentación el socio nos dio luz verde para poder seguir trabajando en este proyecto sin comentario alguno acerca de cambios a realizar aunque por otro lado nos mencionó que le había gustado el aspecto de la aplicación tanto colores como la interfaz.





Finalmente tuvimos un último contacto con Kairen al momento de enviar el Acta Constitutiva del proyecto.



Identificación de ataques informáticos y métodos de ciberseguridad

Las medidas de seguridad implementadas en nuestra aplicación fueron aplicadas gracias a Firebase de Google, que es un almacenamiento de datos en la nube que le permite al administrador escribir sus propias reglas de seguridad. Mediante la autenticación de los usuarios y la administración de reglas de seguridad, es posible manejar los accesos a nuestra base de datos en Firebase.

La seguridad de Firebase se basa en reglas del lado del servidor, que el administrador crea y
establecen los accesos de lectura y escritura a rutas determinadas en nuestra estructura de datos de Firebase. Las reglas de seguridad de Firebase son similares a las de JavaScript, que son sencillas de escribir que permiten el acceso a las credenciales de conexión y a la estructura de datos existente.

La autenticación de Firebase permite un almacenamiento seguro de los datos de nuestros usuarios. Esta autenticación funciona mediante un sistema de tokens: toma datos del usuario para identificarlos, validarlos, para posteriormente pasarlos de forma segura a Firebase para que no se puedan falsificar.