

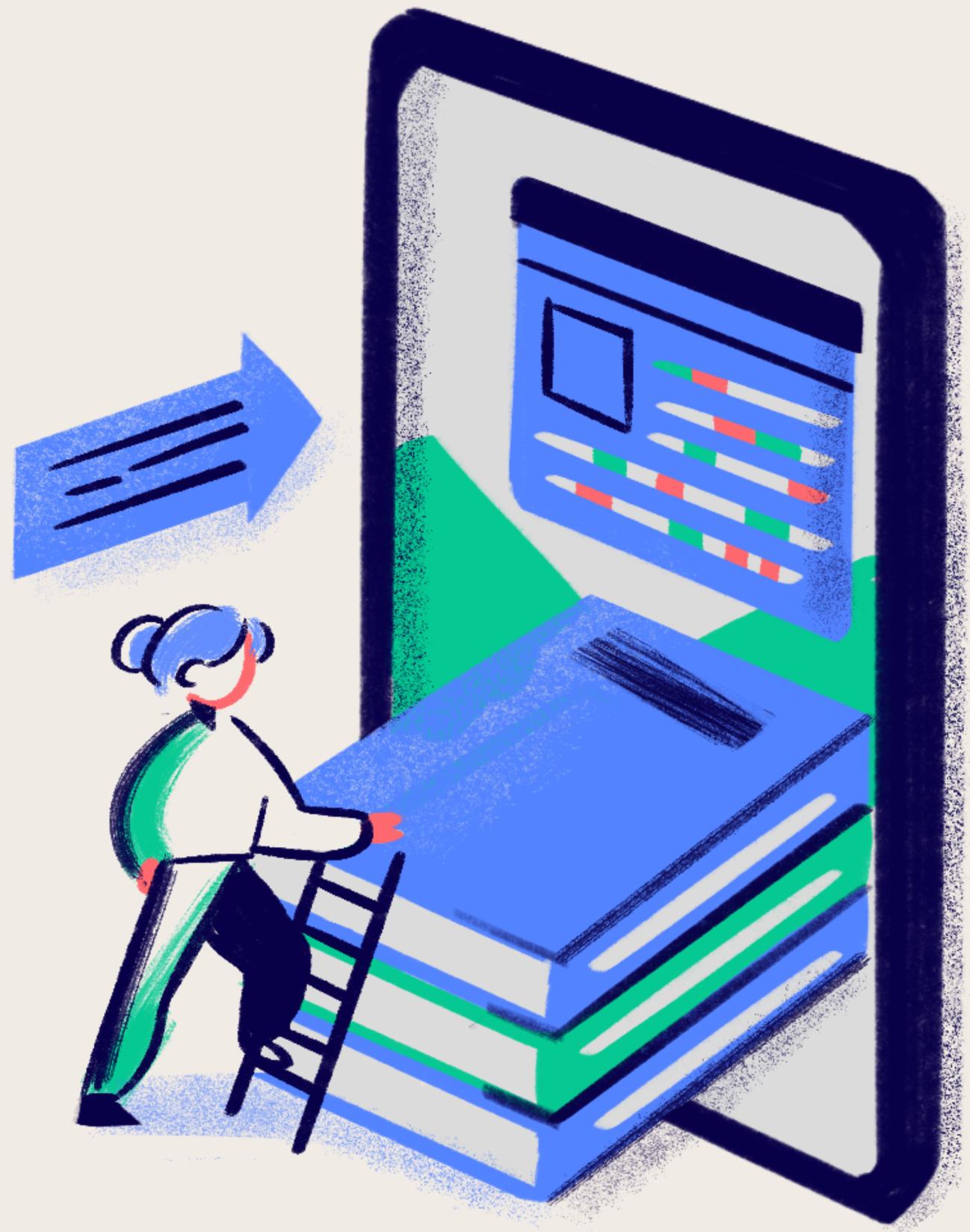
SELECTED TOPICS IN CRYPTOGRAPHY

TOP SECRET RESEARCH PROJECTS

PROPUESTA DE SOLUCIÓN

EQUIPO D:

- FRANCO OLVERA DEMIAN ODER
- OLMO VERDIN DIEGO
- ROMERO HERNÁNDEZ OSCAR DAVID



CONTEXTO

La tecnología ha facilitado la compartición de información a través de la red, pero también ha aumentado los riesgos para la información sensible.

No es viable confiar en la seguridad que un solo individuo pueda proporcionar. De esta manera, la criptografía surge como una solución efectiva para proteger esta información, distribuyendo la responsabilidad y limitando el acceso a datos confidenciales.



PROBLEMA

El gobierno de un país desarrolla proyectos científicos en varias áreas. Cada equipo de investigación tiene dos líderes responsables, pero estos líderes son descuidados con la seguridad digital. La documentación de cada investigación se almacena en un servidor dedicado y se debe cifrar. Para evitar que una sola persona tenga la clave, el gobierno considera usar el intercambio secreto, que divide una clave maestra en fragmentos. Así, varias personas deben reunirse para recuperar la clave. Cada persona almacena su fragmento protegido en su celular, y cada equipo tiene una clave maestra diferente.



ADVERSARIOS

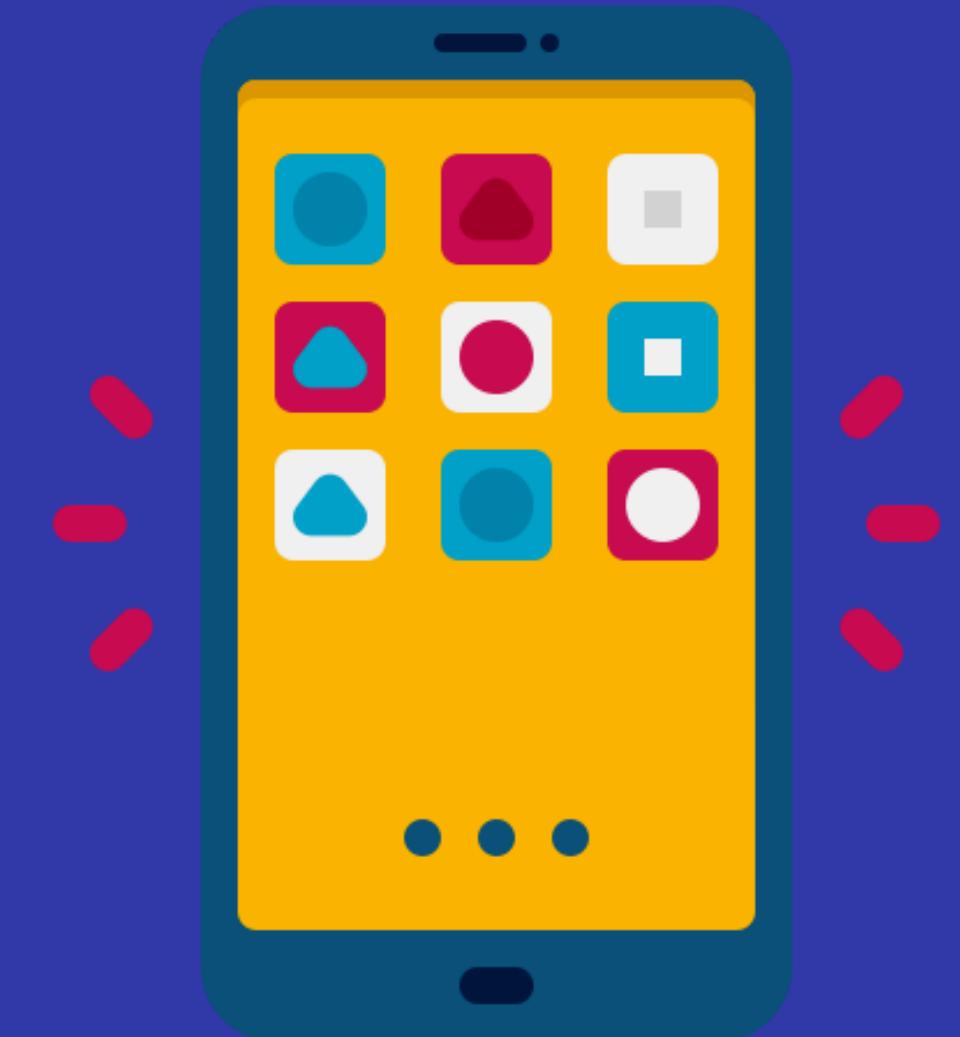
Insiders malintencionados

Personas dentro
del equipo de
investigación o
del gobierno que
tengan
intenciones
maliciosas.

Hackers Externos

Personas que
intenten
acceder al
servidor donde
se almacena la
documentación.

PROPUESTA DE SOLUCIÓN



Para resolver el problema, propone un App móvil que interactúa con una API REST, la cual usa el esquema Secret Sharing de Shamir con EC, que divide una clave maestra en fragmentos. Cada líder de equipo tendrá un fragmento en su celular, y solo un grupo específico de líderes podrá reunir suficientes fragmentos para reconstruir la clave maestra y acceder a la información que quieran cifrar.

TABLA DE SERVICIOS

Servicio Criptográfico	Algoritmo	Seguridad en bits
Confidencialidad	AES	128, 192, 256 bits
Integridad de los Datos	SHA - 256	256 bits
Autenticación	Algoritmo de Shamir	256 - 512 (depende de la curva)

ESTADO DEL ARTE

Entre la principal competencia de nuestra solución propuesta, se encuentran los siguientes programas y aplicaciones móviles de software



NordLocker®



01.

AxCrypt

Programa de tanto de ordenador como móvil que ofrece cifrado de archivos, cifrado y descifrado colaborativo que se implementa con tecnologías de la nube.

02.

Boxcryptor

Programa disponible en escritorio y móvil enfocado en el cifrado en conjunto con tecnologías basadas en la nube como el almacenamiento.

03.

NordLocker

Software de escritorio desarrollado por Nord Security que se enfoca en el cifrado en el entorno de la nube.

CALENDARIO DE ACTIVIDADES (CONSIDERAR 6 CLASES CONTANDO HOY)

JUNIO DE 2024						
LUNES	MARTES	MIÉRCOLES	JUEVES	VIERNES	SÁBADO	DOMINGO
		✓		✗		
3	4	✗	✗	✗		
10	11	✗	✗			
17	18					
24	25					

CALENDARIO DE ACTIVIDADES (CONSIDERAR 6 CLASES CONTANDO HOY)

- 29/05/2024

Avance en la presentación incluyendo documentación, análisis y diseño del proyecto.

- *31/05/2024

Entrega de la presentación con todas las características pedidas (Portada, Contexto, Problema, Adversarios, Propuesta de solución, Tabla de servicios/algoritmo/seguridad en bits, Estado del arte, Calendario de actividades, Requerimientos funcionales, Requerimientos no funcionales, Herramientas a utilizar, Arquitectura, Mockups).

- 04/06/2024

Corrección en la planeación de actividades, así como evaluación de la herramientas a usar en la realización del proyecto.

CALENDARIO DE ACTIVIDADES (CONSIDERAR 6 CLASES CONTANDO HOY)

- 05/06/2024

Inicio del proyecto: Pruebas en AES

- 07/06/2024

Continuación del proyecto, pruebas en la implementación de el algoritmo Shamir.

- 11/06/2024

Continuación del proyecto, creación de la API con la implemetacion de la criptografía propuesto y creación de las pantallas.

- 12/06/2024

Proyecto terminado.

REQUERIMIENTOS FUNCIONALES

- RF1 - Creación de equipos: el sistema permite a un líder de equipo crear un equipo e integrar a otros usuarios.
- RF2 - Generación de clave maestra: el sistema permite a un líder de equipo generar una clave maestra para los equipos que gestiona.
- RF3 - Fragmentación de la clave maestra: el sistema fragmentará todas las claves maestras generadas usando Secret Sharing.
- RF4 - Distribución de los fragmentos: el sistema le enviará los fragmentos creados a cada líder de equipo.
- RF5 - Protección de los fragmentos: los fragmentos están protegidos por una contraseña única que le llega a cada usuario.
- RF6 - Envío de fragmentos y documento: el sistema recibirá los fragmentos y el documento a cifrar por parte de los líderes.
- RF7 - Reconstrucción de la clave: el sistema utilizará Secret Sharing para reconstruir la clave original con los fragmentos recuperados.



REQUERIMIENTOS FUNCIONALES

- RF8 - Cifrado del documento: con la clave maestra reconstruida, el sistema cifrará el documento implementando AES-256.
- RF9 - Almacenamiento del documento: el sistema podrá almacenar en la nube todos los documentos cifrados.
- RF10 - Devolución del documento: el sistema permitirá a los líderes de equipo recuperar su documento cifrado a través de sus fragmentos.
- RF11 - Integridad del documento: aplicando el algoritmo SHA-256, se corroborará la integridad del documento en cada acción realizada.



REQUERIMIENTOS NO FUNCIONALES

RNF1 - Disponibilidad: el servicio estará disponible el mayor tiempo posible para los usuarios.

RNF2 - Escalabilidad: el servicio deberá ser capaz de aceptar más líderes y documentos de presentarse la necesidad.

RNF3 - Rendimiento: la comunicación entre el sistema y sus respuestas tendrá un tiempo razonable de por medio.

RNF4 - Seguridad: Los algoritmos criptográficos utilizados son los más recientes y actualizados.

RNF5 - Usabilidad: el sistema será fácil de comprender para sus usuarios.

RNF6 - Mantenimiento: el sistema será fácil de sostener y actualizar.



HERRAMIENTAS A UTILIZAR

- Frontend - Android Studio (Views)
- Backend - Flask
- Bibliotecas en python para cifrado, descifrado, uso de curvas elípticas



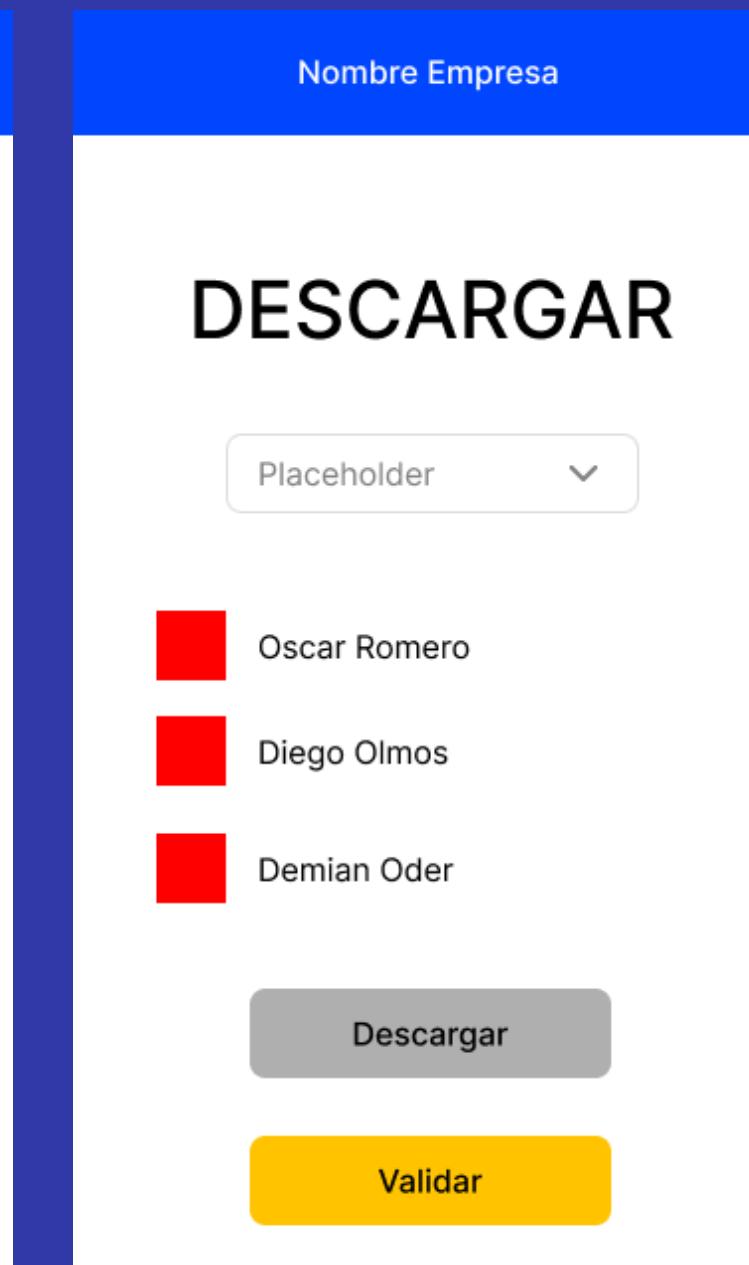
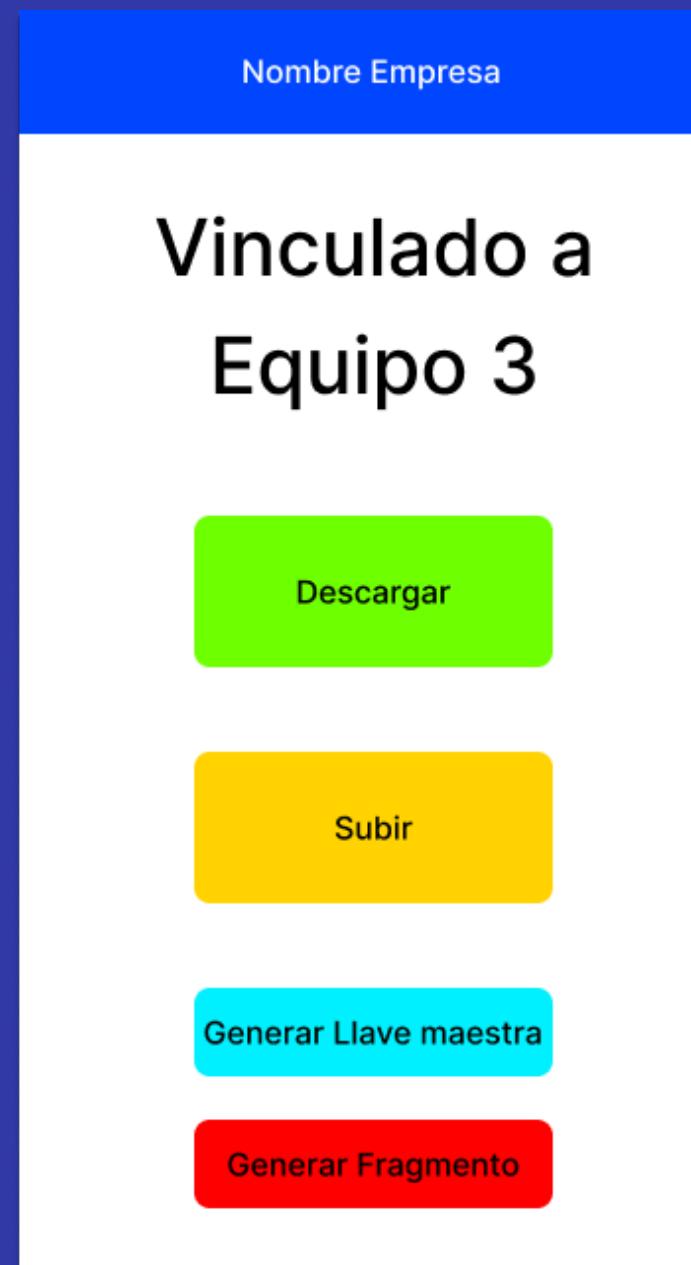
ARQUITECTURA - USUARIOS



ARQUITECTURA - SERVIDOR



MOCKUPS



**GRACIAS
POR SU
ATENCIÓN**

