

**Reflexión individual**

Adrián Eduardo Treviño Peña

21 de Octubre del 2023

Integración de seguridad informática en redes y sistemas de software (Gpo 405)

David Alonso Cantú Delgado

Alberto Ruiz

En este reto se vieron diferentes conceptos de Cyber seguridad, en los cuales nos dieron la iniciativa para implementar estos conceptos dentro de nuestra aplicación de iOS para que nuestros usuarios estén seguros dentro de nuestra aplicación. Esto se nos hizo importante ya que el no hacerlo podría ser un peligro para nuestros usuarios, las organizaciones que trabajarían con nosotros, y nuestra propia información personal y si nosotros no tomamos la responsabilidad de hacer desarrollo de software seguro, la gente involucrada podría tener su información personal robada, utilizada de manera ilícita e incluso podría terminar en algunos siendo extorsionados por esta información.

En el mundo de la ciberseguridad hay leyes, estándares y normas que son aplicadas para que todas las

empresas y/o aplicaciones protegen la información de sus usuarios y de los desarrolladores.

En cuanto a leyes. Esta por ejemplo la Ley Federal de Ciberseguridad en México. En la cual se requiere que el gobierno Mexicano haga cosas como:

“

- Garantizar la seguridad nacional mediante la defensa del espacio digital.

- Crear un marco legal que permita sancionar o tipificar los ciberataques.

- Realizar pruebas de penetración o pentesting anualmente a las instituciones públicas y privadas.

- Crear una Agencia Nacional de Ciberseguridad controlada por el Ejecutivo, similar a los modelos seguidos por la Unión Europea, Estados Unidos y Brasil.

”

(deltaprotect , 2023)

Y en el lado de estándares para empresas tenemos el ISO 27000 el cual sirve para que las empresas de software protegían los datos de sus usuarios.

Esta serie de estándares, leyes y normas son necesarias para proteger a los ciudadanos de México (y potencialmente el mundo si es que otros países implementan algo similar) ya que sin estas leyes y estándares, los usuarios de cualquier software estarían en riesgo de ser privados de su derecho a la privacidad, extorsionados por su información e incluso atacados por fines monetarios y/o políticos.

Hay muchas cosas que reflejan esta serie de estándares y normas que como creadores de software podríamos implementar, desde contratos, implementaciones en los servidores y buenas practicas en el codigo para que la experiencia de todos los involucrados (usuarios, organizaciones y los desarrolladores) sea mas segura. Pero antes de explicar que cosas hicimon en cuanto a seguridad, me gustaria explicar un poco acerca de la estructura de la aplicación entera (frontend y backend).

La aplicación en cuanto lo frontend esta hecha con swift, mientras que en el backend esta hecha con golang y un framework llamado fiber. Este backend se conecta a una base de datos de mongodb y tanto el backend como la base de datos de mongodb estan en un servidor de linux en una maquina virtual del Tecnologico de Monterrey.

Ahora con estas cosas en mente, voy a explicar algunas de las cosas que implementamos en cuanto a ciberseguridad y que cosas no implementamos por tiempo y/o por presupuesto que seria bueno implementar en el futuro.

**Usuarios**

Algo que también tuvimos en cuenta incluso antes de empezar a desarrollar el reto es “El derecho a la intimidad” en el cual se declara que:

“La intimidad es el conjunto de circunstancias, cosas, experiencias, sentimientos y

conductas que un ser humano desea mantener reservado para sí mismo, con

libertad de decidir a quién le da acceso al mismo, según la finalidad que persiga,

que impone a todos los demás la obligación de respetar y que sólo puede ser

obligado a develar en casos justificados cuando la finalidad perseguida por la

develación sea lícita”. (orden jurídico, 2020)

Por esta misma razón tuvimos como enfoque el anonimato. El hecho de que nadie pueda saber quien esta haciendo las búsquedas que esta haciendo amenos que el usuario desee darnos mas información para el mejor funcionamiento de la aplicación.

Otra cosa en la cual no intentamos enfocar es la encriptacion de la información para prevenir que alguien pueda ver lo información de un usuario o de una búsqueda. Es por esto que integramos certificados SSL, lo cual convierte las llamadas http de nuestro servidor a llamadas https y encripta la información desde que sale del dispositivo del usuario hasta llegar al servidor.

**Organizaciones**

Al momento de trabajar con las empresas se les pidió acceso a cierta información de su cuenta de Instagram para sincronizar el contenido de la organización dentro de nuestra aplicación de manera automática. Pero como medida de seguridad de la información, se nos pidió firmar un NDA en el cual se declaraba el uso seguro de esta información.

**Desarrolladores**

En el caso de nosotros los desarrolladores también se utilizo nuestra información personal durante el desarrollo de la aplicación en el código; Ya sea para mandar correos al administrador, contraseñas de aplicaciones, etc. Para mantener nuestra información segura, utilizamos “variables de entorno”, las cuales se utilizan para poder utilizar información personal en tu código sin tener que escribirla para que al momento de publicar el código alguien no pueda verla al analizar el código. En estas variables de entorno teníamos información personal como, e-mails, contraseñas y urls de la base de datos.

**Errores de seguridad de la aplicación**

**Dummies**

en la aplicación utilizamos “dummies” para cuando no teníamos desarrollado la conexión con el backend los cuales consistían en un usuario dummie y una organización dummie. En el caso de la organización dummie, esta tenia el url de una organización real para sacar los datos de su cuenta de Instagram (los posts) y aunque estos no eran datos privados de la organización. Lo correcto hubiera sido el crear una cuenta de Instagram falsa para estos tests.

**Certificaciones no legitimas**

Como Dije en la sección anterior, utilizamos certificaciones ssl para que lo información este encriptada. Pero como la certificación es auto firmada (creada por el mismo servidor) y no es firmada por una certificación legitima, esta aparece como pagina web “no segura”. Lo correcto habría sido comprar una certificación de una empresa legitima y usar ese en nuestro servidor.

**Conclusiones**

De este proyecto yo me llevo que incluso para las personas que no van para lo ciberseguridad. Es muy importante aprender las tecnicas de desarrollo seguro. Ya que de esto va a depender la seguridad de los datos de las y los Mexicanos. Y esta seguridad de los datos tendra (si es que no tiene ya) un impacto de manera nacional y global y todo dependerá de como manejemos estos temas de seguridad en el futuro.

**Referencias**

(N.d.). Retrieved from <http://www.ordenjuridico.gob.mx/Congreso/pdf/86.pdf>

Rivera, S. F. (2023). Retrieved from https://www.deltaprotect.com/blog/ley-de-ciberseguridad-mexico