Librepass

Informe técnico

Un trabajo presentado para la materia de
Emprendimiento Local y Desarrollo Productivo

Krapp Ramiro

Instituto tecnológico San Bonifacio
Departamento de electrónica
29 de junio de 2022

Hecho en LaTeX

Introducción

Librepass es un sistema de seguridad FOSS (Free and Open Source) implementado en base a un sistema de lectores RFID, y con implementación en la nube.

Este está pensado para ser instalado en las puertas de las empresas en las que se desea implementar una seguridad extra, y evitar la entrada de personas no deseadas a ciertas habitaciones, o en todo caso, a la planta entera.

Esta diseñado para ser sencillo de usar e implementar, y presenta un sistema sencillo de niveles de autorización que permite agregar complejidad al sistema de forma que se vea necesaria.

Para su instalación, se provee un set de lectores y tarjetas con cantidad a elección.

Ventajas del producto

El producto presenta múltiples ventajas, en las cuales se incluyen:

- Sencillez a la hora de instalarlo.
- Sencillez a la hora de configurarlo.
- Sencillez a la hora de usarlo.
- Precio económico.
- Escalabilidad
- Cumplimiento de las 4 libertades esenciales del software libre:
    1. La libertad de correr el programa como se desee, para cualquier propósito
    2. La libertad de estudiar cómo el programa funciona, y cambiarlo para que haga lo que el usuario desee. El acceso al código fuente es una precoindición para lograr esto
    3. La libertad para redistribuir copias así puedes ayudar a los demás.
    4. La liberta de distribuir copias de tus versiones modificadas a otros. Haciendo esto, le puedes brindar a toda la comunidad una chance de beneficiarse de tus modificaciones. El acceso al código fuente es una precoindición para lograr esto

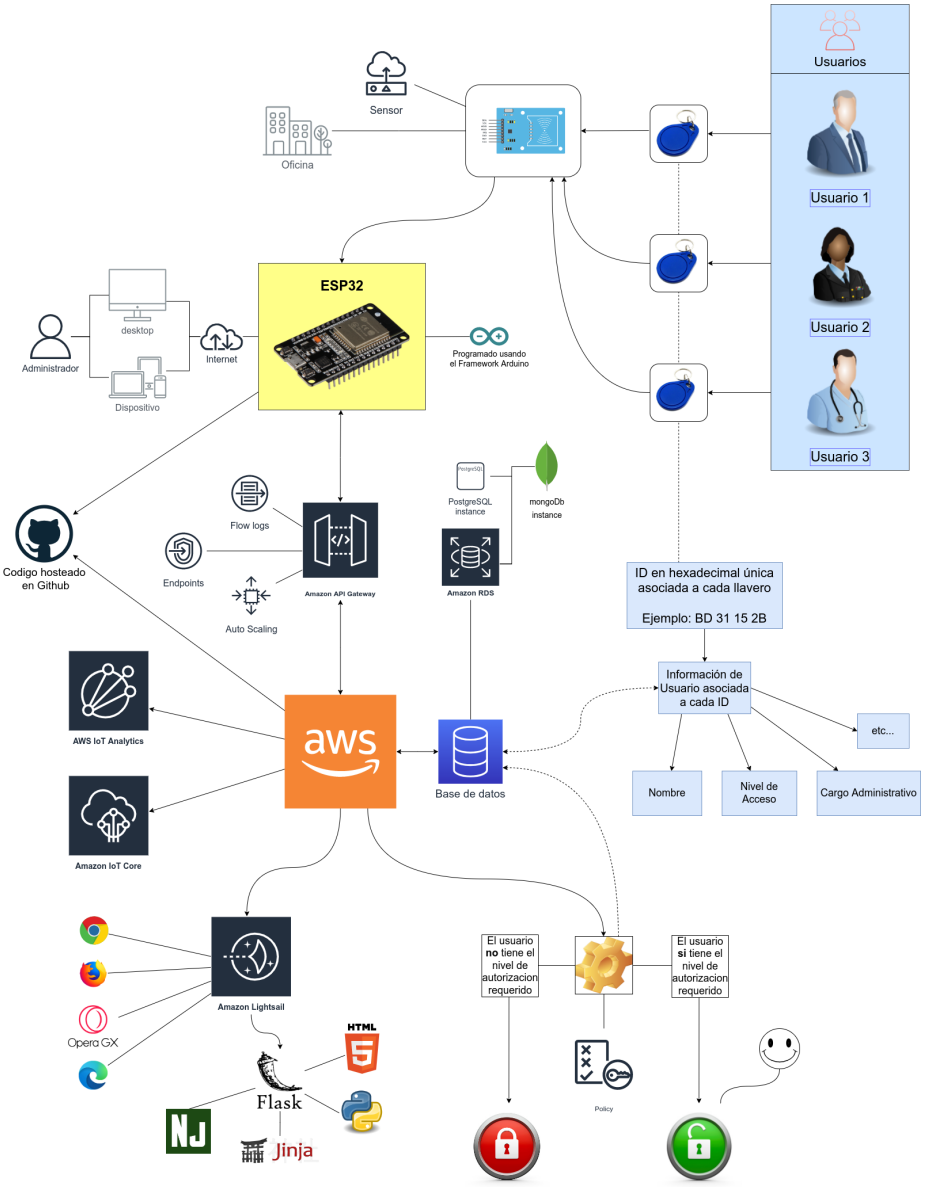

Figura 1: Un diagrama del modelo

Aplicaciones alternativas de la tecnología

Esta tecnología se puede aplicar y modificar para los siguientes usos:

- Un sistema de indentificación de identidad de animales domésticos.
- Un sistema de registro de ingreso y egreso

Resultados de las encuestas

De las encuestas se pueden notar multiples cosas:

1. La tendencia de edad está entre los 18 y 60 años. Esto quiere decir que no hay un grupo etario muy marcado

2. Es notable como la mayoría de los entrevistados tiene cierto conocimiento de los programas de código abierto. Esto se cree que puede ser porque los entrevistados buscaron en internet que eran los programas de codigo abierto, y al hacerlo se enteraron que usaban multiples programas del estilo, como VLC, Firefox, Blender, OBS Studio, qBitTorrent, Audacity, etc...

3. Se le suele dar una importancia notable a la seguridad en las empresas. Esto quiere decir que nuestro producto es relevante. Tambien se ve una gran sensacion de necesidad del aumento de la seguirdad.

4. Es claro como las personas buscan que los sistemas sean sencillos de usar y tambien se busca que de muchas opciones a la hora de configurar, y, en contraste, se dio que hay una buena cantidad de personas que piden que sea minimalista. De esto se puede concluir de que se pueden incluir dos posibles opciones en la configuración: Una que sea un modo sencillo, y otro avanzado, como se hace en las BIOS de ASUS con su EZ Mode

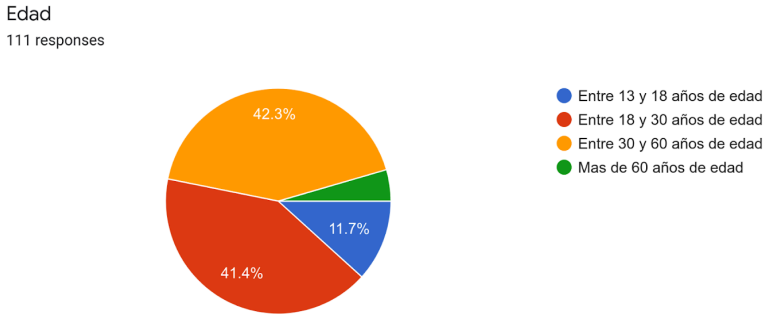

Figura 2: Se puede notar como la tendencia de edad está entre los 18 y 60 años

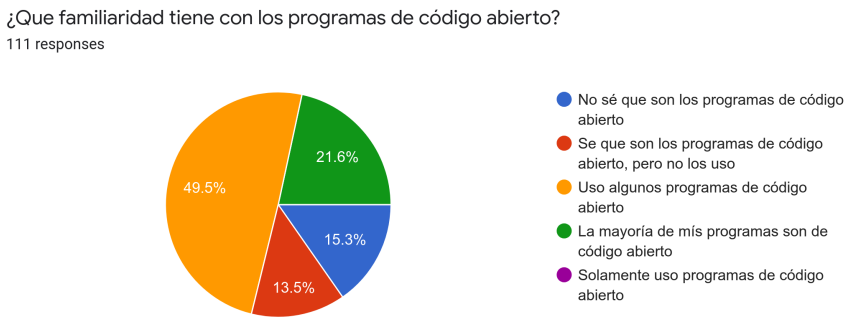

Figura 3: Se puede notar cómo la mayoría de las personas usa algunos programas de código abierto

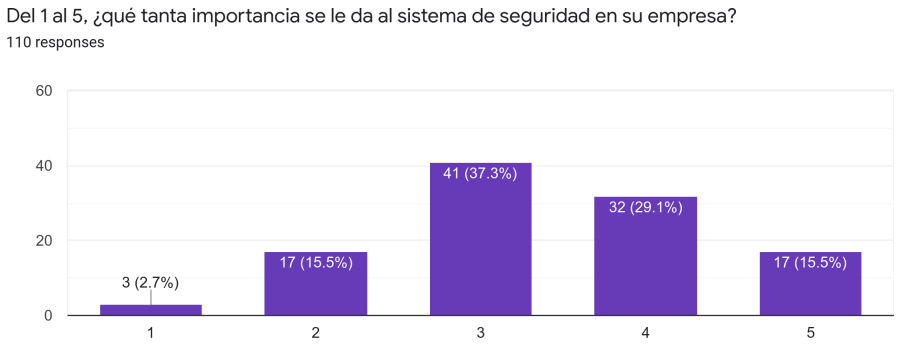

Figura 4: Se puede notar como la importancia hacia la seguridad en las empresas es una campana de Gauss corrida a la derecha

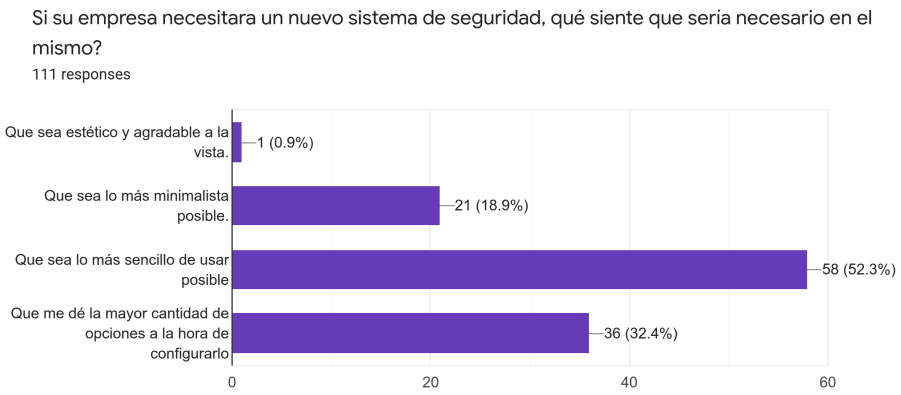

Figura 5: Se puede notar como la mayoría de las personas buscan que sea lo más sencillo de usar

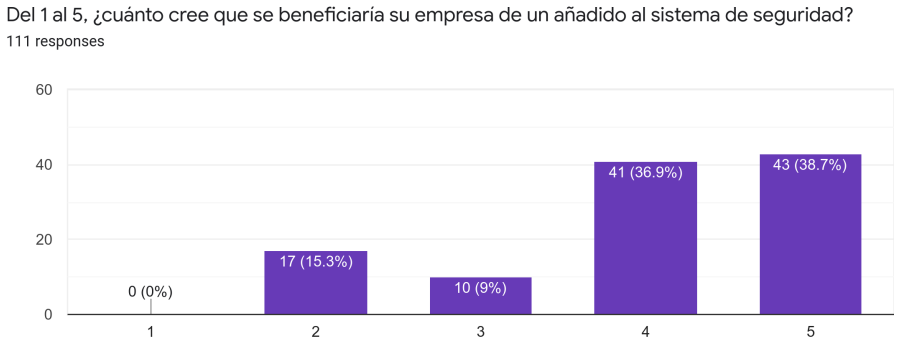

Figura 6: Es evidente cómo las personas creen conveniente un añadido al sistema de seguridad de sus empresas

Resultados de las entrevistas

Entrevistado Numero 1

Nombre

Marcos

Profesion

NodeJs Developer

Edad

24 años

Hace cuanto trabaja en el area de sistemas/programacion?

Si cuento desde que doy cursos (mi primer trabajo formal), diria que desde fines del 2018, y mi primer trabajo como programador fue mayo del 2019

Tiene estudios universitarios?

Analista Universitario en Sistemas de Informacion

¿Tiene experiencia con los sistemas cloud? ¿Qué opina de ellos?

Si, tengo bastante experiencia. Hace un tiempo que vengo trabajando con soporte cloud, en mi experiencia laboral use Firebase y AWS, y en el ámbito personal use Heroku. En si me parece que el termino se hace mucha propaganda porque es algo nuevo, pero en realidad el concepto es algo que ya existía, el alquiler de servidores.

El cloud en realidad es la computadora de otra persona, lo que no había es a nivel estratosférico que hay hoy en día de las grandes empresas. Lo que tampoco había era el sistema de micro servicios de hay hoy en día.

Lo que tiene de ventajoso el cloud es que la otra alternativa, hacer tu propio servidor es algo caro, y nunca le vas a poder ganar a google o a amazon en su capacidad de "hosting", entonces es mucho más barato. Ademas permite hacer el sistema más expansible.

En mi empresa el cloud nos permitió que en casos como en la noche, se pueden des escalar los servicios, y permite tener un uso más económico del servicio, por lo cual es más flexible.

Hoy en día cualquier programador necesita saber lo básico de cloud.

¿Considera que los sistemas cloud son seguros?

Eso depende. Son tan seguros como vos los configures, obviamente se pueden hacer cosas muy seguras, dependiendo que tanto pagues también. Los sistemas muy seguros son caros.

Hay una desventaja también en los sistemas cloud, que es la situación "que pasa si google/amazon se funden", lo cual, como programadores, creemos que es muy poco probable.

Además, los datos de cloud están en el extranjero, lo cual legalmente los pone en una situación distinta. Esto ya pasó con MegaUpload. Por ejemplo, el banco central no les permite a los otros bancos tener datos de los clientes y transacciones en sistemas cloud, por una cuestión legal, para evitar eso. O sea, nosotros en los bancos usamos cloud, pero los datos sensibles están en data-centers acá en argentina. Lo que ponemos en cloud son las aplicaciones, los micro servicios, el backend, algunas bases de datos de utilidad (logs)

En el tema de seguridad, usamos Auth0, la cual es uno de los unicornios argentinos, y nos provee a nosotros los Tokens para los servicios.

¿Tiene experiencia con el mundo del IoT?

No demasiada.

¿Considera que el IoT es seguro?

Es tan seguro como lo configures. El dispositivo IoT debería ser solamente un intermediario de los datos, y no para almacenarlos.

¿Cuando piensa en sistemas de seguridad, que ejemplos se le vienen a la cabeza?

Sistemas de autenticación y/o autorización de acceso de datos y servicios.

¿Qué considera que tiene que tener un sistema de seguridad para ser bueno?

Si pensamos en seguridad fisica, se estila usar politicas de seguridad, como tarjetas de acceso, camaras de seguridad, reconocimiento biométrico.

En seguridad de sistemas, se estila usar tokens de autenticacion y 2FA. Lo que tiene de bueno el 2FA es que las contraseñas suelen ser inseguras, pero el 2FA soluciona eso añadiendo una capa extra de seguridad.

Alguna otra cosa que quieras comentar?

Para tu proyecto, te convendria crear una REST API en heroku e ir consultando a un endpoint, como para empezar.

Conclusiones de la entrevista

Convendria hacer el desarrollo inicial en Heroku, para luego hacer el deploy de produccion a AWS. Es buena la opción de usar cloud, ya que permite usar mejor el sistema monolítico, y es más barato. No es conveniente almacenar datos sensibles en cloud (como datos bancarios), y el servicio cloud debería estar bien configurado. Es conveniente crear una REST API.

Entrevistado Numero 2

Edad

22

Hace cuanto trabaja en el area de sistemas/programacion?

Desde el 2015

Tiene estudios universitarios?

No, pero hice la secundaria técnica en Informática y Redes

¿Tiene experiencia con los sistemas cloud? ¿Qué opina de ellos?

Si, tengo 2 años de experiencia manejando tecnologías cloud, y en el tiempo recorrido he notado la necesidad de implementación de este tipo de tecnologías para agilizar la arquitectura sobre el desarrollo de las distintas aplicaciones y el tiempo de desarrollo de las mismas.

¿Considera que los sistemas cloud son seguros?

Depende de quien los maneje, y el tipo de configuración. Eso depende de como configures el servicio de S3 de Amazon, ese lo podes configurar que sea publico, y si lo agarra alguien que no tenga mucha experiencia y lectura en el tema puede ser bastante inseguro, por eso hay que estar bien informado, el que hace la arquitectura tiene que ser alguien con experiencia.

¿Tiene experiencia con el mundo del IoT?

Si, confio plenamente en la automatización de las cosas del hogar, cualquier cosa que me haga hacer menos, bienvenido sea. Como buen programador, puedo pasar 2 horas automatizando tareas de 10 minutos.

Por ejemplo, en casa tengo todas las luces las tengo conectadas a un switch wifi con el asistente de google, y tengo configurado para que se pueda cambiar el color, la intensidad, horarios de encendido y apagado, etc...

¿Considera que el IoT es seguro?

No, en lo absoluto, en lo más mínimo. Por algo los especialistas en seguridad informática no tienen nada automatizado en la casa

¿Cuando piensa en sistemas de seguridad, que ejemplos se le vienen a la cabeza?

Alarmas, cámaras de seguridad, sensores de movimiento, VPN's, VPC (conecta dos subnets que no estan conectadas al internet exterior, esto se suele hacer en cloud) y sistemas de entrada usando RFID.

¿Qué considera que tiene que tener un sistema de seguridad para ser bueno?

Multiples factores de autenticación y backups de respaldo en caso de perdida de datos y/o energía.

Alguna otra cosa que quieras comentar?

Para la base de datos, podrias usar mongoDB o PostreSQL. En AWS podes usar el servicio EC2

Conclusiones de la Entrevista

Hoy en dia son cada vez más requeridos los sistemas cloud. Estos son seguros dependiendo de que tan bien se configuren, y por lo general la arquitectura la hace alguien con experiencia. Un buen sistema de seguridad debería tener multiples factores de autenticación y backups de respaldo en caso de perdida de datos y/o energía. Para la base de datos, podria usar mongoDB o PostreSQL. En AWS puedo usar el servicio EC2