Interrogantes.

**1. ¿Cuál es el alcance que tienen los sensores de movimiento?**

Un sensor de presencia o sensor de movimiento es un dispositivo electrónico que pone en funcionamiento un sistema (encendido o apagado) cuando detecta movimiento en el área o ambiente en el que está instalado. Se utilizan con frecuencia para optimizar el consumo y la [eficiencia energética](https://www.solerpalau.com/es-es/blog/eficiencia-energetica-en-edificios/) de diversos sistemas como la ventilación, la iluminación o el aire acondicionado en el hogar o en la oficina, aunque también tiene aplicaciones en el ámbito de la seguridad.

Formas de regulación

Independientemente de lo anterior, debemos saber que los sensores de presencia permiten también distintas formas de regulación. Así:

* Pueden ser regulados en relación con el **alcance en metros** para que no interactúen en zonas fuera de su ámbito de actuación porque no interesa o no conviene. Este tipo de regulación es conveniente y utilizada frecuentemente, por ejemplo, en las entradas de las casas.
* Pueden regularse **en función del tiempo** que se desee que se activen desde que detectan un cuerpo hasta que dejen de funcionar. A través de esta opción se pretende optimizar su uso y buscar la máxima eficiencia. De la misma forma, el aparato o sistema que esté conectado a un sensor programado en función de un tiempo determinado, permanecerá conectado solo el tiempo que se estime necesario, controlando de esta forma su [consumo energético](https://www.solerpalau.com/es-es/blog/casas-pasivas/).
* Se pueden regular también en función de la **luminosidad**. Algunos detectores de presencia son crepusculares y se puede optar porque funcionen exclusivamente por la noche, o por el día.
  1. **¿Qué tipo de sensores de movimiento se tienen a la disposición en nuestro país?**

**Sensor de movimiento con campana inalámbrica.**

**Descripción.**

Este sensor es especial para utilizarlo en negocios o comercios. Detecta cuando alguien entra en el establecimiento y envía una señal inalámbrica para que la campana adicional suene y puedas atender a tu cliente de forma oportuna.

El sensor también tiene alarma audible y detecta movimiento hasta 7 m. Colócalo en la entrada del comercio y direcciónalo gracias a su base giratoria.

La campana inalámbrica incorpora múltiples tonos y 3 intensidades de volumen, puedes instalarlo a una distancia de hasta 50 metros del sensor.

Se puede configurar en 2 modos: que solo suene el sensor de movimiento o que suenen el timbre y el sensor.

Fabricado en plástico ABS resistente en color blanco.

**Modulo detector de movimiento de 12v-24v.**

Descripción:

Este módulo contiene un sensor Piroeléctrico, el cual puede detectar cambios de radiación infrarroja. Todo objeto (o cuerpo humano) emite cierto nivel de radiación, y entre mayor temperatura tenga, mayor radiación emitirá. Como respuesta lógica cambia el nivel lógico de un pin, lo que facilita su integración a cualquier sistema. Una de sus principales aplicaciones es la detección de presencia de personas.

* **Tamaño:** Aproximadamente 76x45x35mm
* **Color:** Negro, como muestra la imagen
* **Distancia de Inducción:** 5 ~ 8 m
* **Ángulo de Inducción:** 120 grados
* **Temperatura de funcionamiento:** -20-60 ℃
* **Entrada:** 12-24V
* **Material:** plástico + metal
* **Corriente de salida:** 8A
* **Consumo de energía estática:** <1W
* **Potencia de salida a 12V:** <96W 24V: <192 W
* **Tiempo de retardo:** 60-120 ms

**Sensor de movimiento PIR HC-SR501**

**Descripción.**

Este módulo contiene un sensor Piroeléctrico, el cual puede detectar cambios de radiación infrarroja. Todo objeto (o cuerpo humano) emite cierto nivel de radiación, y entre mayor temperatura tenga, mayor radiación emitirá. Como respuesta lógica cambia el nivel lógico de un pin, lo que facilita su integración a cualquier sistema. Una de sus principales aplicaciones es la detección de presencia de personas.

* Voltaje de operación: 4.5V ~ 20V DC
* Consumo de corriente en reposo: <65 mA
* Salida TTL: 3.3V (alto) / 0V (bajo)
* Ajuste de retardo: 3 ~ 5 min
* Rango de detección: 3 ~ 6 m
* Rango de censado: 120°
* Dimensiones: 32 x 24 x 18 mm

**Control de encendido de luz con sensor de movimiento.**

**Descripción.**

* **Material** Plástico
* **Marca** General eléctrica
* **Aplicación** Interior
* **Tipo de uso** Domestico
  1. **¿Qué tipo de conexión se utilizaría para la comunicación de la aplicación móvil a los sensores?**

Para la aplicación móvil de los sensores se utilizará conexión wifi.

**¿Cómo funciona la conectividad WiFi?**

El **WiFi** se basa en ondas de radio, exactamente igual que la propia radio, la telefonía móvil o la televisión. Por lo tanto, las redes WiFi transmiten información por el aire utilizando ondas de radio.

Ahora bien, las frecuencias que se utilizan para esta tecnología de conectividad inalámbrica son distintas, concretamente **2,4 GHz** hasta el estándar 802.11 n y **5 GHz en**802.11 ac. Actualmente, aunque los 5 GHz proporcionan unas prestaciones superiores, se utilizan ambas frecuencias y, además, en los equipos de mayores prestaciones se combina la transferencia de datos por ambas bandas.

Por lo tanto, cuando vamos a descargar un archivo o solicitamos cierta información a través de una red WiFi, nuestro router recibe los datos de Internet a través de nuestra conexión y posteriormente los convierte en ondas de radio. De esta manera, el router emite estas ondas y el dispositivo inalámbrico que ha solicitado la descarga de ese archivo o información, **las captura y decodifica.**

Ahora bien, estas ondas pueden ser interrumpidas por ciertas **interferencias** causadas por otras redes WiFi o por diferentes aparatos electrónicos como hornos microondas, neveras, televisores o teléfonos inalámbricos, entre otros. De ahí que se insista siempre en analizar bien dónde vamos a colocar nuestro router en casa para tener la mejor conexión inalámbrica posible y evitar ciertas interferencias

* 1. **¿Qué medio se utilizaría para la carga y descarga de datos sobre estado actual de los sensores?**

**Para la carga y descarga de datos se utilizará un servidor web.**

**Servidor web**

Un servidor web es un software que forma parte del servidor y tiene como misión principal devolver información (páginas) cuando recibe peticiones por parte de los usuarios.

En otras palabras, es el software que permite que los usuarios que quieren ver una página web en su navegador puedan hacerlo.

* 1. **¿Qué parámetro se tomará en cuenta para la programación de los sensores de movimiento?**

El parámetro que se tomara en cuenta para la programación depende del lugar en donde serán colocados los sensores.

**6. ¿Qué tipo de mecanismo de cerraduras es más segura para el proyecto?**

El mecanismo más seguro para nuestro proyecto sería la cerradura sobreponer uno de los sistemas de seguridad confiables en nuestro presente, esta cerradura la modificaremos con un solenoide eléctrico para poder implementar de esta forma una parte de los funcionamientos de las cerraduras inteligentes usando los métodos de wifi para mandar una señal apertura al solenoide eléctrico.

* 1. **¿Qué tipo de material es más seguro para crear una cerradura?**

El tipo de material es un poco relativo ya que las cerraduras normalmente son creadas con metal o materiales más resistente para así no ser forzadas y dar acceso a los lugares que queremos proteger, diciendo eso estaríamos usando cerraduras con material de metal.

* + 1. **¿Cuál es el tamaño apropiado para que una cerradura sea segura?**

Generalmente las medidas de entrada, los diámetros de los agujeros son más constantes. El diámetro hecho en la puerta para instalar cerradura es de 54 milímetros (2 1/8 pulgadas) mientras que el agujero hecho para el pestillo de cierre es de 25 milímetros (1 pulgada).

* + 1. **¿Con que mecanismos contara la cerradura para su apertura?**

Usaremos el mecanismo de la cerradura sobreponer, dada con llaves físicas modificando la cerradura para implementar el solenoide eléctrico para poder decidir qué mecanismo usar por uno mismo, queriendo usar ambos o individuales.

* + 1. **¿Por cuales medios adquiriría el usuario la aplicación móvil?**

Los métodos para que los usuarios o clientes adquieran la aplicación móvil puede ser de varias formas como estas mediante correo electrónico, mandando la aplicación en forma apk como también un instructivo para facilitar la instalación de la aplicación en su dispositivo móvil, también como creando una pagina web donde este publicado nuestra cerradura como también la aplicación para su descarga directa desde el navegador al dispositivo otra forma es también es publicar la aplicación móvil en las tiendas oficiales de los teléfonos inteligentes como la Play Store, App Store como también tiendas de terceros también de móvil como Aptoide.

**11 ¿Qué lenguaje de programación e IDE es más apropiado para poder realizar la aplicación móvil que utilizará nuestro prototipo para su funcionamiento?**

En su última actualización 2019, el índice Tiobe, un indicador elaborado por una empresa de software holandesa que se especializa en la evaluación y seguimiento de la calidad de los programas informáticos ha contemplado un nuevo ranking referido a los lenguajes de programación más usados en la actualidad.

Según el portal de internet de Universai.es “La empresa holandesa revisa en tiempo real más de 300 millones de códigos de diversos programas informáticos por día actualizando mes a mes su índice que se elabora a partir de diversas variables, entre las cuales podemos destacar:

* El número de ingenieros cualificados en determinado lenguaje.
* Las búsquedas que hacen los usuarios a través de los buscadores solicitando información de los distintos lenguajes de programación
* La demanda de cursos o los lenguajes que están siendo más utilizados.”

Debemos de recordar la importancia de comprender qué, el índice Tiobe no indica cuál es el mejor o en qué lenguaje de programación se escribió la mayor cantidad de líneas de código. Más bien sirve para que un programador pueda determinar si sus conocimientos en un determinado lenguaje han quedado obsoletos, o si por el contrario sus conocimientos están vigentes.

De acuerdo con estudios realizados los lenguajes más utilizados para programar en orden de mayor a menor serían:

1. Java
2. C
3. Phyton
4. C++
5. C#
6. Visual Basic.Net
7. JavaScript
8. PHP
9. Swift
10. Sql

**12 ¿Qué compatibilidad tendrá la aplicación móvil con los sistemas operativos Android disponibles?**

La pregunta formulada anteriormente se responde con facilidad en demasía, para que nuestra aplicación tenga el mejor funcionamiento y tomando en cuenta que también esperamos tener en el futuro muchas más mejoras respecto a la aplicación y su uso, tendrá una combatividad con Android 4.4 (KitKat) hacia adelante, tomando en cuenta aún a modelo que están siendo antiguos todavía.

Debido a que Android es un proyecto de código abierto, cualquier fabricante de hardware puede crear un dispositivo que ejecute el sistema operativo Android. Sin embargo, un dispositivo es "compatible con Android" solo si puede ejecutar correctamente aplicaciones escritas para el *entorno de ejecución de Android*.

Como desarrollador de apps, no tenemos que preocuparnos acerca de si un dispositivo es compatible con Android, ya que solo los dispositivos que lo son incluyen Google Play Store. Por lo tanto, podemos estar seguro de que los usuarios que instalan tu app desde Google Play Store están usando un dispositivo compatible con Android.

Sin embargo, debemos considerar si nuestra app es compatible con cada posible configuración del dispositivo. Como Android se ejecuta en una gran variedad de configuraciones de dispositivos, algunas funciones no están disponibles en todos los dispositivos. Por ejemplo, es posible que algunos dispositivos no incluyan sensor de brújula. Si la funcionalidad principal de nuestra app requiere el uso de un sensor de brújula, la app solo es compatible con dispositivos que lo incluyen.

La página oficial de desarrolladores de Android nos menciona “Android es compatible con una variedad de funciones que tu app puede aprovechar a través de las API de la plataforma. Algunas funciones están basadas en hardware (como un sensor de brújula), otras están basadas en software (como los widgets de apps) y otras dependen de la versión de la plataforma. No todos los dispositivos son compatibles con todas las funciones, por lo que es posible que debas controlar la disponibilidad de tu app para los dispositivos según las funciones que requiera tu app.”

“Para lograr la mayor base de usuarios posible para tu app, debes esforzarte por ofrecer compatibilidad con tantas configuraciones de dispositivos como sea posible usando un solo APK. En la mayoría de las situaciones, puedes hacerlo inhabilitando las funciones opcionales en tiempo de ejecución y proporcionando recursos de la app con alternativas para diferentes configuraciones (como distintos diseños para distintos tamaños de pantalla).”

Android se ejecuta en diferentes dispositivos con diferentes tamaños y densidades de píxeles de pantalla. El sistema realiza escalamiento y modificación de tamaño básicos para adaptar tu interfaz de usuario a diferentes pantallas, pero aún hay trabajo por hacer a fin de garantizar que tu IU se adapte correctamente a cada tipo de pantalla.

**13. ¿Qué tipo de permisos solicitaría la aplicación al usuario para el funcionamiento de esta?**

Desde Android 6.0 nuestro sistema operativo cuenta un administrador de permisos. Todas las aplicaciones deben solicitar acceso a los distintos elementos del móvil como por ejemplo el micrófono, la ubicación, los contactos o el acceso a los archivos del móvil. Lo que antes era automático, desde hace unos años está mejor controlado, separado y queda bajo nuestro criterio el permitir que las aplicaciones puedan tener determinados permisos.

Administrar los permisos de Android es algo que todos deberíamos conocer ya que es una manera sencilla de mejorar nuestra seguridad y privacidad. Lo que ocurre es que Android dispone de bastantes más permisos de los que pensamos. Y es que además de los permisos normales como acceder a la cámara o a los SMS, también existen varios permisos avanzados que acceden a datos sensibles y con capacidad para modificar elementos clave de Android.

Vamos a explicar qué tipo de permisos podemos encontrarnos, qué riesgos conlleva aceptarlos y qué tipo de apps acostumbran a solicitarlos. Al finalizar de presentarlos, estaremos indicando que permisos necesitaría nuestra aplicación para el correcto funcionamiento de todas las funciones.

Los primeros permisos que debemos controlar son los más básicos, pero no por ello menos importantes. Aquí se engloban los que normalmente suelen solicitar las aplicaciones tradicionales como redes sociales o herramientas. Algunos ejemplos serían; el almacenamiento que sirve para poder adjuntar archivos, micrófono para poder enviar notas de voz, contactos para recomendarnos amigos o SMS para comprobar tu número de teléfono.

Nuestra aplicación no tendría la necesidad de pedir información de contactos, ni de SMS ni de voz, etcétera, ya que no es una aplicación que dependa realmente de estos permisos como lo son las redes sociales que si dependen de tener esta información para su correcto uso y funcionamiento.

Otro tipo de permisos son los de accesibilidad. En las nuevas versiones de Android se ha mejorado mucho este aspecto y precisamente gracias a estas opciones muchos usuarios pueden controlar el móvil sin que su discapacidad sea un impedimento. Para ello se añaden opciones de control por voz, lectura de textos y demás opciones donde aplicaciones concretas pueden acceder a información que de otra manera no sería posible.

¿Qué es lo que ocurre? Básicamente que muchos desarrolladores aprovechan el potencial del permiso de accesibilidad para su aplicación. En este caso sobre todo para detectar cuando se activa una aplicación en concreto y actuar en consecuencia.

Podríamos pensar en utilizar unos de estos permisos para la aplicación que necesitamos, sin embargo, no depende del todo de estos, ya que no necesitaríamos saber tan exigentemente que un usuario esté utilizando una aplicación específica o algún otro apartado del teléfono. En dado caso para futuras actualizaciones se podrían tomar en cuenta algunos cambios en la misma y poder solicitar algunos de los permisos de accesibilidad, dejándolo a la consideración del usuario y sin afectar el uso de esta con los permisos que necesitamos originalmente.

Otro permiso que algunas aplicaciones solicitan es el acceso a notificaciones. ¿Para qué? Básicamente para poder mostrarnos estas notificaciones de una manera distinta. O incluso poder acceder a estas notificaciones y trasladarlas a otro dispositivo, como es el caso de las aplicaciones relacionadas con los wearables (relojes o bandas inteligentes).

Es un permiso importante, ya que tener acceso a las notificaciones no solo implica poder mostrarlas, también llegar a leerlas y actuar en función de lo que ponga escrito. Este permiso a levantado mucha controversia por la posibilidad que tienen las aplicaciones cuando el usuario autoriza el permiso, ya que la aplicación en cuestión puede tener acceso a las notificaciones del teléfono, no solo para mostrar o ver notificaciones, sino también para poder editarlas y leerlas.

Este permiso sería sumamente importante para nuestra aplicación, ya que implica tener informado al usuario de lo que está sucediendo a la distancia con su cerradura, recordemos que todo funcionará por medio de una nube en la cual estaremos subiendo y bajando datos de forma continua y los cuales tienen que ser presentados al usuario para cualquier inconveniente que pueda suceder.

El usuario estará completamente en la disposición de poder rechazar este permiso, sin embargo, este será muy necesario para el uso de la aplicación y poder estar enterado de que está pasando minuto a minuto con su cerradura.

Algunas aplicaciones solicitan acceder a nuestras notificaciones para poder funcionar, como sería el caso de la nuestra. Un permiso que implica un riesgo elevado por la cantidad de información sensible que se suele mostrar en ellas, pero, es por ello que hay que tener en consideración los términos y condiciones de uso del usuario para que pueda estar tranquilo de por qué y para qué se utilizaría el permiso requerido.

Otro acceso de permiso especial es el de datos no restringidos. Se trata de un permiso muy especial donde ninguna aplicación debería tener acceso. Sí la solicitan los 'Carrier Services' y los 'servicios de Google Play', como vemos, dos aplicaciones de Google muy integradas y que se mantienen para poder acceder a los datos en el momento que sea necesario. Normalmente está relacionado con servicios de emergencia y alertas.

Este último también es muy importante, puesto que nuestra aplicación se utilizaría también como servicio de alertas y avisos sumamente importantes, ya que al saber que hay movimiento o alguien intentó abrir la cerradura, se tiene que indicar en el momento al usuario para que pueda tomar una decisión o en dado caso, poder ver que acción realizará para poder observar lo que sucede con su cerradura.

El listado de permisos especiales es bastante largo y va desde los servicios de ayuda de RV, acceso a SMS premium o el acceso de optimización de batería, para evitar que una aplicación quede en segundo plano.

Sí hay uno de ellos que queremos repasar. Es el permiso de administrador de dispositivos. Se trata de uno de los más potentes y permite realizar acciones que en muchas ocasiones están reservadas para usuarios con acceso root. Con este permiso las aplicaciones podrán bloquear la pantalla, eliminar todos los datos o inhabilitar el bloqueo de pantalla. Es importante revisar qué aplicaciones tienen acceso a ello porque es el más importante.

Este permiso es sumamente sensible, y únicamente aplicaciones totalmente certificadas como pueden ser las aplicaciones de Google es recomendable darles acceso, nuestra aplicación no necesitaría este permiso, pero lo mencionamos ya que nuestra cerradura tendría un sistema similar a la utilización de este permiso, lograr cerrar el candado desde tu celular y poder desbloquearlo únicamente utilizando un patrón o contraseña que únicamente el usuario podrá saber.

En nuestros dispositivos móviles llevamos datos muy personales que no nos gustaría que una aplicación maliciosa nos robara. Para evitar disgustos lo mejor es siempre descargar aplicaciones de sitios de confianza como Google Play, donde apenas se cuela el malware. O de sitios web en dónde esté colocado todo lo relacionado al uso de los mismos, para que puedas tener confianza de la aplicación que estarás utilizando y que estará revisando constantemente las notificaciones que puedan llegar a ingresar acerca de la integridad de nuestro prototipo.

**14. ¿Con qué métodos de seguridad (Ejemplo: ¿Pin, huella, etc.) contaría la aplicación móvil para acceder a ella?**

Hay diferentes tipos de características de seguridad de las aplicaciones, como la autenticación, la autorización, el cifrado, el registro y las pruebas de seguridad de las aplicaciones.

Como nos indica la página VM Ware, que es una web especializada en seguridad en informática: “Los desarrolladores de software pueden integrar procedimientos de autenticación y autorización en las aplicaciones para asegurarse de que solo accedan los usuarios autorizados. Los procedimientos de autenticación garantizan la identidad de los usuarios. Se consigue obligando a los usuarios a proporcionar un nombre de usuario y una contraseña para iniciar la sesión en una aplicación. La autenticación multifactor requiere más de una forma de autenticación. Por ejemplo, algo que el usuario sabe (una contraseña), algo que tiene (un dispositivo móvil) y algo que le caracteriza (una huella dactilar o el reconocimiento facial).”

Lo que buscamos y queremos lograr con nuestra cerradura es que el usuario se sienta seguro de tenerla colocada en su casa, negocio o apartamento, y lo vamos a lograr teniendo algunos métodos de autenticación requeridos para poder manipular la cerradura al gusto del cliente.

Queremos colocar un máximo de 3 usuarios para cerradura o colocar más en algún caso especial, que pudiera ser alguna familia con un número elevado de personas, pero la idea principal es cerrar el rango de personas que puedan manipular esta cerradura para no arriesgar la integridad del usuario.

Agregaremos un login, que será para registrar al usuario con su cerradura y ligarlos directamente en la nube para poder empezar a manipularla desde su dispositivo Android.

Luego queremos lograr utilizar alguna autenticación extra nativa de el dispositivo que se esté utilizando, podría ser una huella dactilar, reconocimiento facial o reconocimiento de iris en algunos otros pocos casos.

Una vez autenticado, puede autorizarse al usuario para acceder a la aplicación y a utilizarla. El sistema puede validar que el usuario tenga permiso para acceder a la aplicación comparando su identidad con una lista de usuarios autorizados. La autenticación se debe efectuar antes que la autorización para que la aplicación solo contraste las credenciales de usuario validadas con la lista de usuarios autorizados.

Cuando el usuario esté autenticado y esté usando la aplicación, queremos proteger los datos confidenciales con otras medidas de seguridad para que los malwares no los vean ni los usen. En las aplicaciones basadas en la nube, en las que el tráfico que contiene datos confidenciales circula entre el usuario final y la nube, ese tráfico se puede cifrar para proteger los datos lo cual se iría realizando en próximas actualizaciones.

Por último, si se vulnera la seguridad de una aplicación, el registro puede ayudar a identificar quién ha accedido a los datos y cómo. Los archivos de registro de la aplicación ofrecen un control con marcas de tiempo de los aspectos de la aplicación a los que se ha accedido y de la persona implicada. Es necesario probar la seguridad de las aplicaciones para asegurarse de que todos estos controles de seguridad funcionen correctamente.

Por otro lado, como nos indica el mismo portal web de VM Ware “La seguridad de las aplicaciones en la cloud plantea desafíos adicionales. Dado que los entornos de nube ofrecen recursos compartidos, se debe comprobar con especial atención que los usuarios solo tengan acceso a los datos que están autorizados a consultar en las aplicaciones basadas en la nube. Los datos confidenciales también son más vulnerables en las aplicaciones basadas en la nube, puesto que los datos se transmiten por Internet del usuario a la aplicación y viceversa.”

También nos brindan información acerca de las aplicaciones móviles y los métodos de autenticación: “Los dispositivos móviles también transmiten y reciben información por Internet, no por una red privada, de modo que son vulnerables a ataques. Las empresas pueden utilizar redes privadas virtuales (VPN) para añadir una capa de seguridad a las aplicaciones móviles que proteja a los empleados que inicien sesión en las aplicaciones de forma remota. Los departamentos de TI también pueden optar por revisar las aplicaciones móviles y asegurarse de que cumplan las políticas de seguridad de la empresa antes de permitir que los empleados las usen en los dispositivos móviles que se conecten con la red empresarial.”

Los controles de seguridad de las aplicaciones son técnicas que mejoran la seguridad de una aplicación a nivel de codificación para que sea menos vulnerable a las amenazas. Muchos de estos controles afectan a cómo responde la aplicación a entradas inesperadas que un ciberdelincuente podría utilizar para aprovecharse de una debilidad. Un programador puede escribir código para una aplicación que le otorgue más control sobre el resultado de estas entradas inesperadas.

Los desarrolladores de aplicaciones realizan pruebas de seguridad de las aplicaciones dentro del proceso de desarrollo de software para asegurarse de que no haya vulnerabilidades de seguridad en una versión nueva o actualizada de una aplicación de software. Las auditorías de seguridad pueden garantizar que la aplicación cumpla una serie específica de criterios de seguridad. Una vez que una aplicación supera la auditoría, los desarrolladores deben asegurarse de que solo puedan acceder a ellas los usuarios autorizados. En las pruebas de intrusión, los desarrolladores piensan como un ciberdelincuente y buscan formas de irrumpir en la aplicación. Las pruebas de intrusión pueden incluir ingeniería social o intentos de engañar a los usuarios para que permitan el acceso no autorizado. Por lo general, los verificadores llevan a cabo análisis de seguridad tanto sin autenticar como autenticados (como usuarios con la sesión iniciada) para detectar vulnerabilidades de seguridad que quizás no se den en ambos estados.

**15. ¿De qué forma alertaría la aplicación móvil al usuario sobre un posible robo?**

Una notificación es un mensaje que muestra Android fuera de la IU de la app para proporcionar al usuario recordatorios, mensajes de otras personas y otra información puntual de la app. Los usuarios pueden presionar la notificación para abrir la aplicación o realizar una acción directamente desde la notificación.

Las notificaciones se muestran a los usuarios en diferentes ubicaciones y formatos, por ejemplo, como un ícono en la barra de estado, una entrada más detallada en el panel lateral de notificaciones o un distintivo en el ícono de la aplicación.

La manera con la que tu dispositivo Android te va a indicar que hay alguna novedad en una de las aplicaciones que tienes instalada es mediante las notificaciones. Estas se mostrarán tanto en la pantalla de bloqueo como directamente en el panel de notificaciones que aparece al deslizar el dedo hacia abajo desde la parte superior izquierda de la pantalla del móvil.

Las aplicaciones pueden mostrar principalmente dos tipos de notificaciones. Algunas son notificaciones no deseadas con promociones o mensajes poco importantes que realmente no tienen mucho que ver con el contenido o lo que está pasando en la aplicación, aunque también pueden servir para aprovechar y mostrarte algunos tipos de recordatorios.

En el caso de nuestra aplicación estaremos utilizando esta función de Android para poder realizar las actividades que son necesarias, como por ejemplo, avisarle al usuario que su cerradura sufrió algún tipo de manipulación o intento de desbloqueo que no fue realizado por el usuario principal, poder notificar quien ingresa o se enlaza a la cerradura de la que es dueña, y/o poder corroborar el estado en el que se encuentra esta.

Actualmente contamos con miles de variantes de Android, ya que cada proveedor modifica el sistema según sus propias necesidades y no siempre para mejor. Pero la base de Android es un sistema operativo bien diseñado y cada vez más seguro con cada nueva versión.

O, mejor dicho, cada vez es más seguro siempre que el usuario haga las cosas bien. Para hacerse con una gran cantidad de datos interesantes en almacenamiento compartido o ganar acceso a una función que pueda ser insegura, las aplicaciones de Android requieren siempre el permiso explícito del usuario; pero es esencial que estos permisos se establezcan correctamente.

En función de como vayamos avanzando con nuestra aplicación, podemos activar otros permisos distintos, como podría ser el caso de la ubicación, para saber si el usuario se encuentra lejos o cerca de la ubicación de su cerradura.

**16. ¿Qué lenguaje de programación es más viable para la parte electrónica del proyecto?**

Arduino

Arduino ofrece una sintaxis de programación intuitiva y esto hace que realizar prototipos sea mucho más fácil.

Cómo funciona Arduino

El Arduino es una placa basada en un microcontrolador ATMEL. Los microcontroladores son **circuitos integrados en los que se pueden grabar instrucciones**, las cuales las escribes con el lenguaje de programación que puedes utilizar en el entorno Arduino IDE. Estas instrucciones permiten crear programas que interactúan con los circuitos de la placa.

El microcontrolador de Arduino posee lo que se llama una **interfaz de entrada**, que es una conexión en la que podemos conectar en la placa diferentes tipos de periféricos. La información de estos periféricos que conectes se trasladará al microcontrolador, el cual se encargará de procesar los datos que le lleguen a través de ellos.

El tipo de periféricos que puedas utilizar para enviar datos al microcontrolador depende en gran medida de qué uso le estés pensando dar. Pueden ser cámaras para obtener imágenes, teclados para introducir datos, o diferentes tipos de sensores.

**17. ¿Qué tipo de conexión se utilizaría para la comunicación de la aplicación móvil a la cerradura y los sensores?**

Para la conexión a internet de la aplicación móvil, la cerradura y los sensores se utilizará conexión WIFI. Hoy en dia es común tener un Router en las viviendas que proporciona señal Wifi para conectar todo tipo de dispositivos electrónicos.

**¿Qué es WiFi?**

WiFi, es una tecnología que permite la **conexión inalámbrica entre dispositivos electrónicos**, ordenadores, smartphones, tablets, televisores, videoconsolas, etc. Wi-Fi es una marca de Wi-Fi Alliance o Alianza Wi-Fi, la organización que promueve dicha tecnología y que se encarga de certificar todos los productos que se ajustan a las normas establecidas de interoperabilidad.

Una tecnología que surgió por la necesidad de establecer una manera de conexión inalámbrica que fuese compatible con distintos dispositivos. Por lo tanto, el objetivo de la Alianza fue diseñar una marca que permitiese fomentar más fácilmente la tecnología inalámbrica y asegurar la compatibilidad entre dispositivos.

**18. ¿Qué IDE es más apropiado para los lenguajes de programación escogidos?**

Para la programación de los sensores y el módulo Wifi se utiliza el IDE de Arduino y para la programación de la Aplicación de Móvil se utiliza Android Studio.

En la internet se encuentra una gran cantidad de documentación para Arduino y esto facilita la creación de unos proyectos de electrónica sin la necesidad de ser un profesional.

**Android Studio.**

Android Studio es el entorno de desarrollo integrado (IDE) oficial para el desarrollo de apps para Android y está basado en [IntelliJ IDEA](https://www.jetbrains.com/idea/). Además del potente editor de códigos y las herramientas para desarrolladores de IntelliJ, Android Studio ofrece incluso más funciones que aumentan tu productividad cuando desarrollas apps para Android, como las siguientes:

* Un sistema de compilación flexible basado en Gradle
* Un emulador rápido y cargado de funciones
* Un entorno unificado donde puedes desarrollar para todos los dispositivos Android
* Aplicación de cambios para insertar cambios de código y recursos a la app en ejecución sin reiniciarla
* Integración con GitHub y plantillas de código para ayudarte a compilar funciones de apps comunes y también importar código de muestra
* Variedad de marcos de trabajo y herramientas de prueba
* Herramientas de Lint para identificar problemas de rendimiento, usabilidad y compatibilidad de versiones, entre otros
* Compatibilidad con C++ y NDK
* Compatibilidad integrada con [Google Cloud Platform](https://cloud.google.com/tools/android-studio/docs/?hl=es-419), que facilita la integración con Google Cloud Messaging y App Engine

**19. ¿Qué Hardware sería más apropiado para el manejo de lo electrónico?**

Para controlar la cerradura y los sensores se utiliza la placa de desarrollo Arduino.

**Arduino.**

Al ofrecer una combinación adecuada de hardware y software de IoT, Arduino es una plataforma de IoT fácil de usar. Opera a través de una serie de especificaciones de hardware que se pueden dar a la electrónica interactiva. El software de Arduino viene en el plan del lenguaje de programación Arduino y el entorno de desarrollo integrado (IDE).

1. **¿Dónde se almacenarán los datos recopilados de los usuarios?**

Los datos de los usuarios junto con los de la cerradura y los sensores, serán almacenados en una base de datos en un servidor Web.

A diferencia de utilizar una servidor Web(API) ya creado, es que el tráfico de datos es menor y esto hace que el envío y descarga de información se en un periodo de tiempo mucho más corto.