UNIVERSIDAD
COMPLUTENSE
MADRID

Proyecto de Innovación Convocatoria 2021/2022

Nº de proyecto: 258

Competencias digitales para el uso del Smartphone en el aula y la seguridad digital: aplicaciones móviles

Aurora Cuevas-Cerveró

Responsable del proyecto

Facultad de Ciencias de la Documentación

Departamento: Biblioteconomía y Documentación

1. Objetivos propuestos en la presentación del proyecto

El objetivo general de nuestro proyecto ha sido promover las competencias digitales del profesorado y alumnado vinculadas a la seguridad informática y al uso del smartphone en el aula estimulando de este modo un empleo didáctico del teléfono móvil y un uso seguro de internet.

Para atender a este objetivo nos propusimos los siguientes objetivos específicos:

1. Identificar las competencias digitales que debemos promover en el profesorado atendiendo a las directrices marcadas por el modelo DigComp (Unión Europea) seguido por las Bibliotecas Universitarias Españolas (REBIUN).
2. dentificar programas que permitan diseñar apps de forma fácil y seleccionar aquél que mejor se adecúe a nuestros fines.
3. Diseñar un curso, siguiendo las especificaciones tecnológicas de una App sobre seguridad informática (nivel usuario).
4. Diseñar un curso, siguiendo las especificaciones técnicas de una App sobre uso didáctico del smartphone en el aula.
5. Sondear la opinión del profesorado y alumnado sobre este tipo de aplicaciones con vistas a una implementación futura de los mismos en el ámbito docente.

2. Objetivos alcanzados

1. Identificar las competencias digitales que debemos promover en el profesorado atendiendo a las directrices marcadas por el modelo DigComp (Unión Europea) seguido por las Bibliotecas Universitarias Españolas (REBIUN).
2. Identificar programas que permitan diseñar apps de forma fácil y seleccionar aquél que mejor se adecúe a nuestros fines.

El modelo DigComp nace en 2010 en el seno de la Comisión Europea, quien a través del Instituto de Prospectiva Tecnológica (IPTS) inicia el desarrollo del marco de competencias digitales para la ciudadanía. La primera versión salió a mitad del 2013 firmado por Anusca Ferrari. Del 2015 al 2016 se contrastó la primera versión y se publicó la versión 2.0 con algunas modificaciones. En 2017 se ha publicó la versión 2.1 y en 2022 la versión 2.2. denominada *The Digital Competence Framework for Citizens - With new examples of knowledge, skills and attitudes.* Este modelo integra las competencias incluidas en la Alfabetización informacional (ALFIN), la alfabetización mediática y las competencias informáticas, además de otras competencias generales o relativas al aprendizaje con medios colaborativos, participativos y sociales. Se trata de un iniciativa cuyo objetivo es Identificar y describir los componentes claves de la competencia digital (DC) en términos de conocimiento, habilidades y actitudes procurando aunar la multiplicidad de iniciativas

dispersas y diversas en un marco común, que incorpore competencias informacionales, digitales, mediáticas y sociales ofreciendo una herramienta para la implementación, medición, desarrollo del currículo, competencias del profesorado, certificación y autoevaluación. Con el valor añadido de ser un marco que no permanece estático, sino que va evolucionando e incluyendo mejoras según se va testando y la sociedad va evolucionando por lo que es altamente indicado para un proyecto de innovación con vocación de servicio al profesorado.

Las competencias identificadas para la seguridad informática corresponden de manera directa a las dimensiones 1 y 2: Seguridad, en concreto los apartados 4.1 (protección de dispositivos) y 4.2 (protección de datos personales y privacidad)

Para la selección y configuración de la app también hemos tomado como referencia el Marco Europeo de la Competencia Digital *DigComp 2.2*, que indica la necesidad de un software de código abierto, en este caso hemos seleccionado *React Native. React Native*, también conocida como *React.js*, es una librería que funciona bajo JavaScript, es el marco de desarrollo multiplataforma, comenzó como una herramienta interna de Facebook para crear componentes de aplicaciones nativas se hizo de código abierto en 2015, como resultado, tiene la reputación de impulsar algunas de las principales aplicaciones móviles a nivel mundial, como Pinterest, Skype, Facebook, Instagram y entre otras. Además, las aplicaciones creadas con esta tecnología ofrecen una experiencia similar a la nativa y está disponible de forma gratuita bajo la licencia MIT (Instituto Tecnológico de Massachusetts) de código abierto.

3. Diseñar un curso, siguiendo las especificaciones tecnológicas de una App sobre seguridad informática (nivel usuario).

Una vez configurada la aplicación se ha distribuido el diseño y elaboración de los contenidos entre los miembros del equipo que ha trabajado colaborativamente a través de la plataforma Google Drive. Se ha tomado en consideración que estamos diseñando contenidos para una app formativa que va dirigida a alumnado y profesorado, desde esta perspectiva los contenidos deben ser rigurosos, pero a la vez breves y sencillos, con elementos textuales y audiovisuales y debe incluir una autoevaluación.

La programación del curso incluye los siguientes módulos: *Contraseñas*, *Copias de seguridad, Protección antivirus, Actualizaciones de software, Cuidado con las WiFi públicas y los cargadores públicos, Desactivación de las redes inalámbricas, herramientas antirrobo, redes sociales y otras alternativas.*

Los contenidos de cada uno de los apartados se han organizado en dos bloques: Amenazas y Protección y consejos de seguridad para smartphones.

4. Diseñar un curso, siguiendo las especificaciones técnicas de una App sobre uso didáctico del smartphone en el aula.

Entre los módulos disponibles, como modelo se eligió *Contraseñas*, el curso llevó por título "Contraseñas y seguridad en Smartphones" (Anexo A). En este sentido, se elaboraron completamente los contenidos referentes a dicho módulo, incluyendo especificaciones de uso, casos prácticos y evaluación. El contenido incluye los siguientes temas: Contraseñas y Seguridad a nivel del Smartphone para Dispositivos Android y Dispositivo iOS. Contraseñas y Seguridad a nivel de apps en el Smartphone Para Android. Usando Google Play Protect para proteger nuestras aplicaciones y la privacidad de nuestros datos. Gestión de contraseñas en Google Chrome para iOS. Para acabar: software para la gestión y creación seguras de contraseñas. Recursos utilizados. Para repasar: preguntas y caso práctico. 6 preguntas y Caso práctico.

5. Sondear la opinión del profesorado y alumnado sobre este tipo de aplicaciones con vistas a una implementación futura de los mismos en el ámbito docente.

La opinión de profesorado y alumnado se ha sondeado sólo de modo informal a partir de una validación de la app realizada con 10 profesores y 10 alumnos. Los resultados iniciales de esta validación indicaron la necesidad de ampliar los contenidos por lo que se solicitó financiación para una ampliación del proyecto denominada "Competencias digitales para el uso didáctico del Smartphone en el aula y la protección de datos personales", ya en curso. En la segunda fase del proyecto está prevista la evaluación de la app a partir de cuestionarios.

3. Metodología empleada en el proyecto

El proyecto se organizó en cuatro fases que a su vez se vinculan a los objetivos iniciales. Cada fase se desglosa en tareas concretas.

- Fase 1. Identificación de competencias: Con el objetivo de Identificar las competencias necesarias que debemos incluir en nuestros contenidos. Se destacaron tres tareas:

Tarea 1. Los profesores participantes y el personal de bibliotecas revisaron el Modelo de Competencias Digitales DigComp verificando la pertinencia de su inclusión en nuestros cursos en función de su vinculación a los ítems, uso seguro de internet y uso didáctico del Smartphone; Tarea 2. Seleccionar las competencias digitales para incluir en nuestro proyecto. Se seleccionaron en función de su importancia y prioridad, de acuerdo a su transversalidad, su especificidad y a su grado de dificultad; y Tarea 3. Informe de seguimiento. Para concretar las tareas fueran realizadas reuniones y seleccionadas las siguientes competencias digitales: protección de dispositivos, protección `de datos personales y privacidad. Creando contenidos informativos de amenazas, protección y consejos seguridad para smartphones.

-Fase 2. Identificación, selección y configuración de software e inclusión de contenidos, el objetivo fue Identificar, seleccionar y organizar los contenidos en el software seleccionado.

También con tres tareas: Tarea 1. Se identificaron aplicaciones de software libre para diseño de apps de uso en teléfonos inteligentes con el objeto de identificar los que se adecuen a nuestros objetivos. Aunque hay varios programas conocidos, se amplió el análisis para verificar que pueda usarse uno de amplio espectro (generalmente este tipo de programas se dirigen al sistema operativo Android, pues iphone tiene un distribuidor de aplicaciones más restringido. Se eligió el framework de apps multiplataforma y de código abierto React Native. Tarea 2. Se impartió un curso de formación a los participantes en su uso, para que a su vez pudiesen implementar los cursos diseñados en la siguiente fase.Tarea 3. Informe de seguimiento.

- Fase 3. Diseño de los cursos. El objetivo fue Realizar el diseño relativo a la estructura de la información y contenido de los cursos. Se destacó por cuatro tareas: Tarea 1. Se trabajó en la estructura para la organización de la información y la inclusión de los contenidos. Tarea 2. Se diseñaron los contenidos para el curso, que incluirán texto, imagen y vídeo. Tarea 3. Búsqueda de ejemplos de buenas prácticas sobre uso didáctico del smartphone en el aula.Tarea 4. Informe de seguimiento.
- Fase 4. Validación. El objetivo fue evaluar los resultados de la app entre profesores y alumnos. Se realizó una validación no formal con una muestra de 10 profesores y 10 alumnos a los que se les mostró el funcionamiento de la app

4. **Recursos humanos** (Máximo 1 folio)

El equipo del proyecto está formado por 10 personas, en el que participan PDI, PAS y estudiantes de postgrado y doctorado, en este último caso pertenecientes a dos facultades distintas (Ciencias de la Documentación y Ciencias de la Información.

Responsable	María Aurora Cuevas Cerveró	PDI Complutense
Miembros	Fabiana da Silva França	Investigadora postdoctorado
	Eliane Pellegrini	Investigadora predoctoral
	Cristina Barrios Martínez	PDI Complutense
	José Antonio Magán Wals	PAS Complutense
	Luis Fernando Ramos Simón	PDI Complutense
	Luis Miguel Cruz López	Estudiante
	Michela Montesi	PDI Complutense
	Pablo Parra Valero	PDI Complutense
	Pedro Lázaro Rodríguez	PDI Complutense

El 45% de los componentes del equipo son PDI pertenecientes al Grupo de Investigación Información, Biblioteca y Sociedad (INFOBISOC) de la Facultad de Ciencias de la Documentación de la UCM, siendo una de sus Líneas de Investigación la Alfabetización

Informacional y la Competencia Digital (https://www.ucm.es/informacionbibliotecaysociedad/).

5. Desarrollo de las actividades

Las iniciativas de acceso abierto permiten la distribución electrónica gratuita de publicaciones que aceleren y enriquezcan la investigación, y que científicos, académicos, investigadores, docentes y estudiantes pueden tener acceso al conocimiento que se produce en las instituciones, sin la necesidad de esperar el envío del material impreso o pagar altos costos por la compra o descargar un elemento. Para cumplir con uno de los objetivos de la investigación: “promover las competencias digitales del profesorado y alumnado vinculadas a la seguridad informática y al uso del smartphone en el aula estimulando de este modo un empleo didáctico del teléfono móvil y un uso seguro de internet", optamos por usar el *framework open source, React* Native orientado al desarrollo de aplicaciones móviles de contenido informativo.

5.1 Selección y configuración de la plataforma App y Elaboración de los contenidos del curso e inclusión en la App

Este proyecto se ha realizado con el framework React Native, mediante la instalación de las herramientas necesarias como instalación de Visual Studio Code (editor de código), Android Studio y librería del React Native. El framework React Native permite desarrollar aplicaciones móviles, tanto para iOS como para Android, con JavaScript y creando la interfaz de usuario de la misma manera que se hace en React. Además, ofrece una serie de componentes nativos, es decir, que se corresponden con componentes en su correspondiente plataforma, que permiten un aspecto visual y rendimiento similar al de las aplicaciones nativas.

Algunas tecnologías del proyecto

Tecnología	Descripción
React-Native	Framework para aplicaciones nativas de IOS y Android.
Expo	Framework para el desarrollo de aplicaciones.
JavaScript	Lenguaje de programación interpretado
NestJS	Framework para el crear aplicaciones del lado del servidor.
TypeScript	Lenguaje de programación tipado

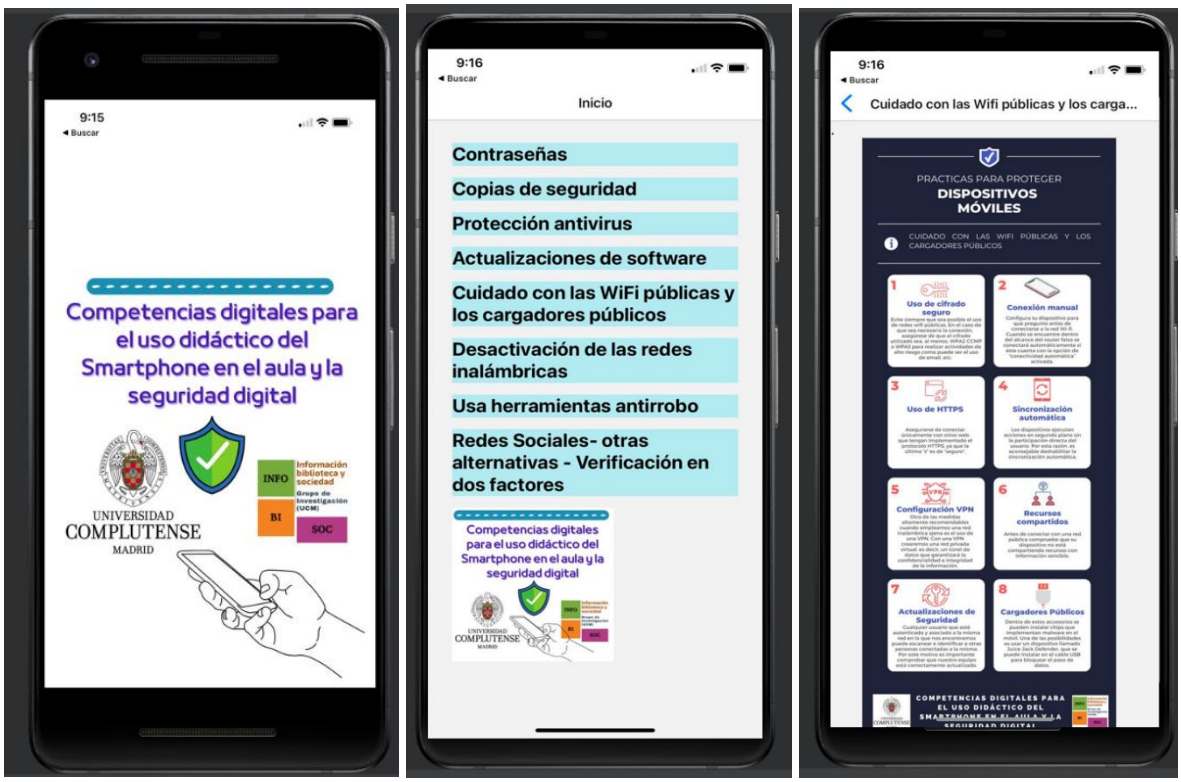
A continuación, se muestra el código del componente dedicado a este propósito, omitiendo algunas partes que no son relevantes en este apartado. De paso, se pueden ver los nombres de las pantallas que han quedado finalmente en la aplicación, y parte de la sintaxis que involucra la creación de componentes.

```
import React from 'react'
import { Text, View, StyleSheet, Image, Button } from 'react-native'
```

```
import { NavigationContainer } from '@react-navigation/native'
import { createNativeStackNavigator } from '@react-navigation/native-stack'

const Stack = createNativeStackNavigator ()

import Home from './screens/home'
import Passwords from './screens/passwords'
import Backups from './screens/backups'
import Dangers from './screens/dangers'
import Updates from './screens/updates'
import Wifi from './screens/wifi'
import Wireless from './screens/wireless'
import Tools from './screens/tools'
import Social from './screens/social'

function MyStack ({ navigation }) {
  return (
    <Stack.Navigator initialRouteName="Home">

      <Stack.Screen
            name="Home"
            component={Home}
            options={{ title: 'Inicio' }}
            initialParams={{ itemId: 42 }} />

      <Stack.Screen
            name="Passwords"
            component={Passwords}
            options={{ title: "Contraseñas - Passwords" }}/>

      <Stack.Screen
            name="Backups"
            component={Backups}
            options={{ title: "Copias de seguridad - Backups" }}/>

      <Stack.Screen
            name="Dangers"
            component={Dangers}
            options={{ title: "Protección antivirus - Dangers" }}/>

      <Stack.Screen
            name="Updates"
            component={Updates}
            options={{ title: "Actualizaciones de software - Updates" }}/>

      <Stack.Screen
            name="Wifi"
            component={Wifi}
            options={{ title: "Cuidado con las Wifi públicas y los cargadores públicos -
Wifi" }}/>

      <Stack.Screen
            name="Wireless"
            component={Wireless}
            options={{ title: "Desativación de las redes inalámbricas - Wireless" }}/>

      <Stack.Screen
            name="Tools"
            component={Tools}
            options={{ title: "Usa herramientas antirrobo - Tools" }}/>

      <Stack.Screen
            name="Social"
            component={Social}
            options={{ title: "Redes Sociales - otras alternativas - Verificación en dos
fatores - Social" }}/>

    </Stack.Navigator>
  )
}
export default function App() {
  return(
    <NavigationContainer>
      <MyStack/>
```

```
    </NavigationContainer>
  );
}
 const styles = StyleSheet.create({
  container: {
    flex: 1,
    justifyContent: "center",
    alignItems: "center",
    backgroundColor: "#ffffff"
  },
}
);
```

La pantalla inicial de la aplicación. Consiste en una pantalla en blanco con el logo creado para la aplicación. Esta se aprovecha también para esperar a que se realicen ciertas cargas antes de mostrar la aplicación. Una vez estas cargas se han completado, la pantalla se desvanece con una transición a transparente, dando lugar a la vista de pestanas con la sección inicial y luego accediendo a cada página por el menú principal.



Enlace para acceder la app: https://expo.dev/@proyectosinnovacion/app-innovacion

Para la verificación y validación de la aplicación se realizó un proceso de test exhaustivo sobre este tipo de sistemas porque es muy complejo. Por una parte, está el inconveniente de que han de funcionar sobre una variedad inmensa de dispositivos distintos, y en dos sistemas operativos distintos también Android y IOS. Por otra, una de las partes más importantes de este proyecto es la interfaz de usuario, y había que lograr que se adapte bien a los distintos tamaños de pantalla sobre los que se va a mostrar. Así, los tests que se han realizado en este proyecto sobre componentes React Native, no han sido realizados de manera tan completa como se podría porques es necesario más tiempo, en otros proyectos sería interesante verlo con más profundidad. Eso se debe al entorno de trabajo es costoso de instalar en cuestión de tiempo y hay muy pocas informaciones a la hora de resolver problemas.

Tras terminar este proyecto de la app en React Native, tenemos una aplicación totalmente funcional y preparada para ser publicada en las Stores de los diferentes sistemas operativos, pero se van a tener en cuenta una serie de mejoras de cara al futuro desarrollo de la aplicación, entre otras añadir más apartados y contenidos más interativos. Como se puede observar en las futuras mejoras, el proyecto va a mejorar bastante de cara a un a la próxima versión de forma que podamos ofrecer una aplicación cada vez más completa dependiendo del feedback que recibamos de los usuarios.

Referencias bibliográficas

Boduch, A. 2017. «React and React Native. Livery Place». 35 Livery Street, Birmingham. Packt Publishing Ltd.

Caballero, J. 2018. «¿Cómo funciona React.js? Página Oficial de DevCode». Fecha de consulta el 15 de febrero de 2022. https://devcode.la/blog/como-funciona-reactjs/.

Fernández Bajón, M. T., Cuevas Cerveró, A., Montesi, M. y Palafox Parejo, M. 2015. «MOOC: guía para la elaboración de Trabajos Fin de Grado y Trabajos Fin de Master en Ciencias Sociales». [Proyecto de Innovación Docente]. https://eprints.ucm.es/id/eprint/28702/.

Gómez-Hernández, J.-A. y Fernández-Rincón, A.-R. 2021. «La sátira gráfica de Calpurnio y El Roto sobre la digitalización social: un análisis crítico desde la perspectiva de las competencias digitales». *Informação &Amp; Sociedade*: Estudos 30, n.º4:1–34. https://doi.org/10.22478/ufpb.1809783.2020v30n4.57792.

Lazcano Calixto, R. N., Valencia González, L. Á., Baena Díaz, D. E. y Venegas Guzmán, R. 2019. «React Native: acortando las distancias entre desarrollo y diseño móvil multiplataforma». *Revista Digital Universitaria* (rdu) 20, n. º 5 septiembre-octubre. http://doi.org/10.22201/codeic.16076079e.2019.v20n5.a5.

Novick, V. 2017. «React Native-Building Mobile *app*s with JavaScript». Birmingham: Packt Publishing Ltd.

Proyecto Innova-Docencia 258. 2021. «Competencias digitales para el uso didáctico del *smartphone* en el aula y la seguridad digital. Proyectos de Innovación 2021-2022». Facultad de Ciencias de la Documentación (UCM).

Pinto, M., Fernández-Pascual, R., Gómez-Hernández, J.A., Cuevas-Cerveró, A., Granell, X., Puertas, S., Guerrero, D., Gómez, C. y Palomares, R. 2016. «Q1 Attitudes toward

Information Competency of University Students in Social Sciences». *Portal: Libraries and the Academy* 16, n. º 4: 737–761. https: //digitum.um.es/xmlui/bitstream/10201/50895/6/project_muse_632343.pdf.

Pinto, M., Gómez-Hernández, J. -A., Sales, D., Cuevas-Cerveró, A., Guerrero-Quesada, D., Fernández-Pascual, R., Caballero, D. y Navalón-Vila, C. 2019. «Aprender y enseñar competencias digitales en un entorno móvil: avances de una investigación aplicada a profesorado y alumnado universitario de Ciencias Sociales». *Revista Ibero-Americana de Ciência da Informação RICI* 12, n. º 2: 585-596. https://doi.org/10.26512/10.26512/rici.v%2012.n2.2019.23590.

Sales, D., Cuevas-Cerveró, A. y Gómez Hernández, J. A. 2020. «Perspectives on the information and digital competence of Social Sciences students and faculty before and during lockdown due to Covid-19». *Profesional de la información* 29, n. º 4. https://doi.org/10.3145/epi.2020.jul.23.

European Commission. Plan de Acción de Educación Digital. 2021-2027. Fecha de consulta el 05 de febrero de 2022. https://education.ec.europa.eu/es/focus-topics/digital-education/digital-education-action-plan.

European Commission's Joint Research. 2022. «DigComp 2.2: The Digital Competence Framework for Citizens - With new examples of knowledge, skills and attitudes». European Union. Fecha de consulta el 10 de noviembre de 2021. https://europa.eu/!cKrmj6.

UNESCO. 2021. «Dejar entrar el sol: transparencia y responsabilidad en la era digital». Fecha de consulta el 10 de noviembre de 2021. https://unesdoc.unesco.org/ark:/48223/pf0000377231_spa.

Vuorikari, R., Kluzer, S. y Punie, Y. 2022. «DigComp 2.2: The Digital Competence Framework for Citizens - With new examples of knowledge, skills and attitudes». EUR 31006 EN, Publications Office of the European Union, Luxembourg. http://dx.doi.org/10.2760/490274.

6. Anexos

ANEXO A – Curso Contraseñas y seguridad en Smartphones

Contraseñas y seguridad en Smartphones

Contenidos

1. Introducción

La seguridad en dispositivos Smartphone depende en gran medida del sistema operativo empleado. No es lo mismo disponer de un Smartphone con Android que de un Smartphone con iOS (un Iphone). En el caso de los Smartphones con Android, sucede también que cada marca o modelo puede tener una estructura de categorías de configuración diferente (por ejemplo, las categorías de configuración pueden variar de nombre en un móvil LG con respecto a un móvil Xiaomi o Motorola). Lo mismo puede suceder en Smartphones con iOS y los diferentes modelos que existen (Iphone 8, 9, 10, 14, etc.). Aún con todo, suelen disponer de las mismas posibilidades aunque se nombren de forma diferente.

De manera general, la seguridad en cuanto a contraseñas y seguridad en Smartphones puede explicarse a dos niveles:

- Seguridad a nivel del Smartphone (del aparato o dispositivo en sí)
- Seguridad a nivel de apps en el Smartphone (por ejemplo en navegadores web, apps de redes sociales, etc.)

En este documento se explican métodos para ganar en seguridad en dichos niveles tanto en Android como en IOS.

Es importante reconocer las fuentes de información de este documento. Para todo lo relativo a Android, se ha utilizado la información disponible en la página web oficial de ayuda de Android. Esta misma página, en una de sus secciones, ofrece información de ayuda de fabricantes diferentes para los dispositivos (sitios web de ayuda de Samsung, LG, Motorola, Pixel y Xiaomi). En cuanto a las fuentes para todo lo relativo a iOS (iPhone), se ha utilizado el manual de la versión 16, aunque en la misma página para dicho manual se puede seleccionar la versión 14 o 15 del sistema.

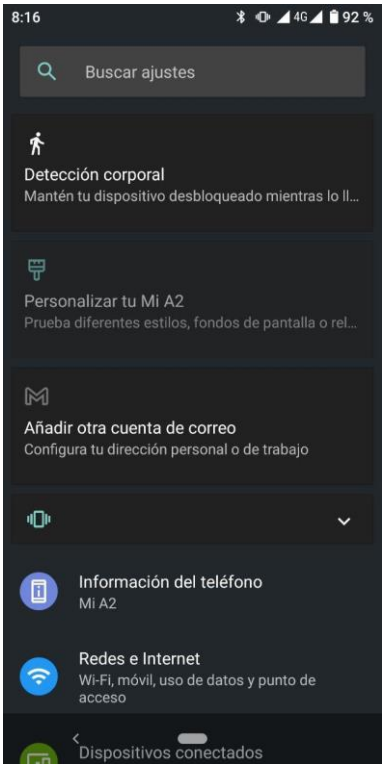
2. Contraseñas y Seguridad a nivel del Smartphone

2.1. Dispositivos Android

En primer lugar, vamos a aprender a configurar el bloqueo de pantalla en un dispositivo con Android. Toda la información de este punto se ha extraído de la sección de la ayuda de Android titulada "Configurar el bloqueo de pantalla en dispositivos Android". Hacerlo es importante para proteger nuestro dispositivo en caso de extravío o robo. Configurar el bloqueo nos obliga a utilizar algún sistema de desbloqueo que solo cada persona individualmente conocemos. De esta forma, si perdemos o nos roban el teléfono, no podrán desbloquearlo a no ser que también conozcan el patrón, PIN o contraseña que hayamos definido para el desbloqueo de la pantalla. El sistema de desbloqueo tiene varias alternativas (por patrón, PIN, contraseña o huella dactilar si el dispositivo cuenta con esta funcionalidad).

Para conocer cómo configurar una opción de desbloqueo, vamos a seguir los siguientes pasos (las capturas de pantalla que sirven de ejemplo han sido realizadas en un móvil Xiaomi MI A2 con la versión de Android 10):

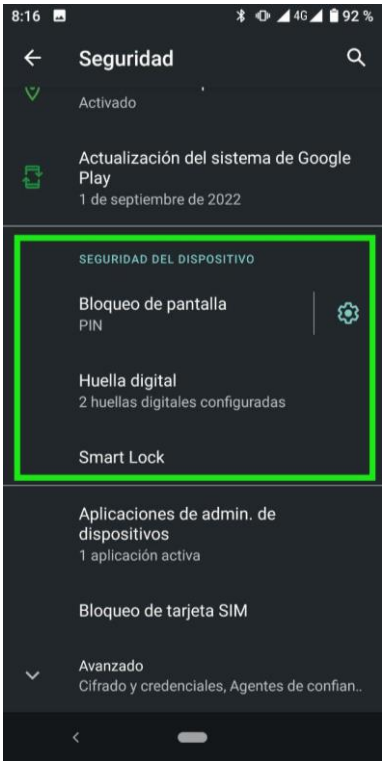
1. Abrimos la aplicación "Ajustes" del teléfono (en la siguiente captura se ve la sección o aplicación de ajustes del teléfono que se toma de ejemplo):



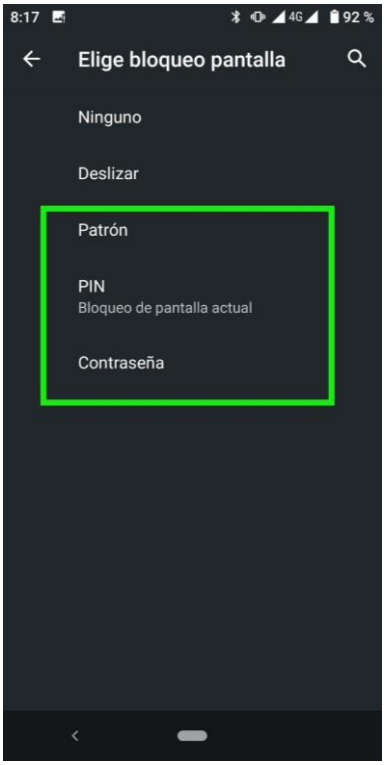
2. Buscamos y accedemos a la sección de "Seguridad":
   - Importante: dependiendo de cada versión de Android o modelo y marca del móvil, este nombre puede variar. Si no vemos "Seguridad", podemos consultar dónde encontrar estos ajustes en el sitio web de asistencia del fabricante del teléfono:

3. Pulsamos ahora en Bloqueo de pantalla para seleccionar un tipo de bloqueo.

- Importante: quizá tuviéramos ya un bloqueo configurado. Si ya teníamos uno configurado, tenemos que introducir el PIN, patrón o contraseña para seleccionar otro sistema de desbloqueo distinto. Dicho de otra forma, una vez que hayamos definido un sistema de desbloqueo, cuando queramos cambiar algo relacionado con la seguridad del teléfono, el mismo teléfono nos lo va a pedir para poder realizar los cambios que queramos.

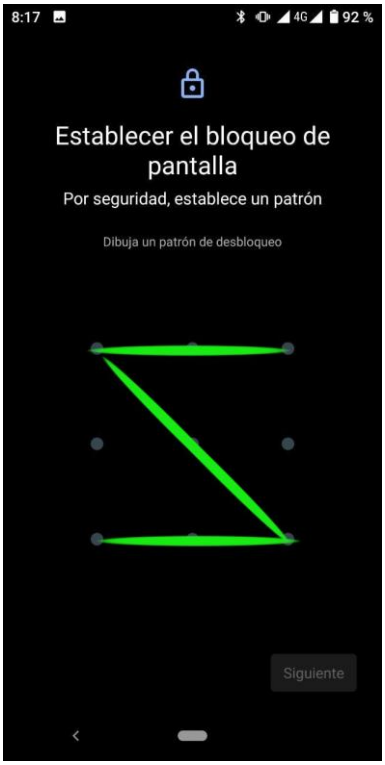


4. Seleccionamos la opción de bloqueo de pantalla que queramos utilizar y seguimos las instrucciones que aparecen en pantalla (importante: la opción de “ninguno” y “deslizar” no son opciones de bloqueo como tal; sí lo son las de patrón, PIN y Contraseña):



Las opciones de bloqueo o tipo de bloqueo dependen en ocasiones del tipo de móvil que tengamos. Quizá hasta tengamos uno que permita la identificación y el desbloqueo con huella dactilar. Estas son las opciones más comunes:

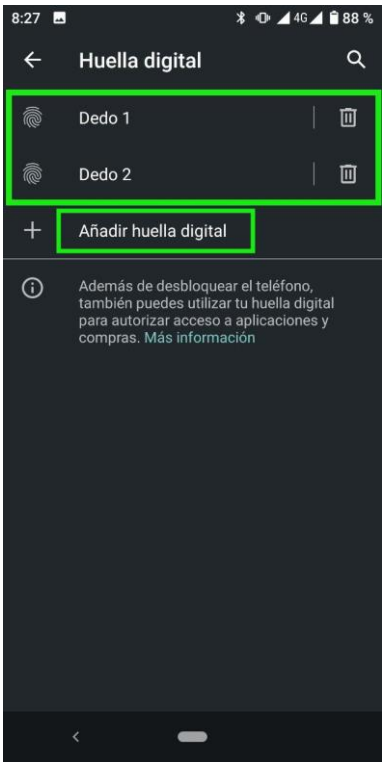
- Sin bloqueo:
  - **Ninguno**: el teléfono permanecerá desbloqueado. Esta opción no ofrece protección, pero podremos acceder rápidamente a nuestra pantalla de inicio.
  - **Deslizar**: se desbloqueará si deslizamos el dedo por la pantalla. Esta opción no ofrece protección, pero podremos acceder rápidamente a la pantalla de inicio.
- Bloqueos estándar:
  - **Patrón**: consiste en desbloquear dibujando un patrón sencillo con el dedo. Esta opción de Patrón nos dejaría dibujarlo y definirlo desde una pantalla similar a la siguiente (la Z en verde de la captura, sería el patrón diseñado y que al dibujarlo en el mismo sentido en que lo definimos, nos permitirá desbloquear el teléfono):



  - **PIN**: consiste en introducir al menos 4 dígitos. Los PIN más largos ofrecen mayor seguridad y sería preferible evitar un PIN del tipo 2222 y similares.

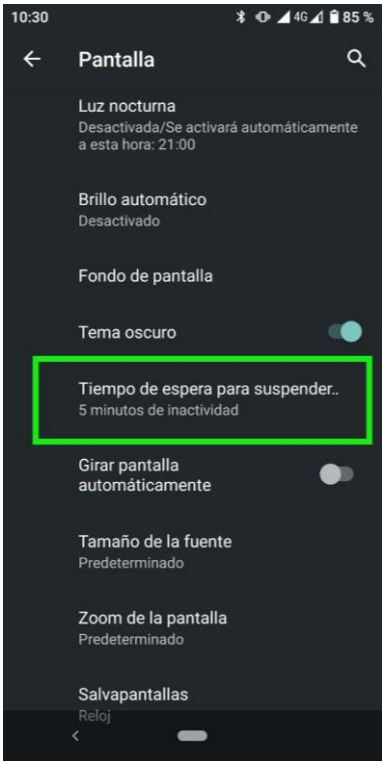
- **Contraseña**: consiste en introducir al menos 4 dígitos o letras. Una contraseña segura es la opción de bloqueo de pantalla que más seguridad ofrece.
  Si nuestro móvil dispone de lector de huella digital, también aparecerá dicha opción. A esta opción se accede desde la sección de seguridad, en concreto en la categoría de "Huella digital", desde donde se puede configurar:

- Se puede añadir incluso más de un dedo o huella:

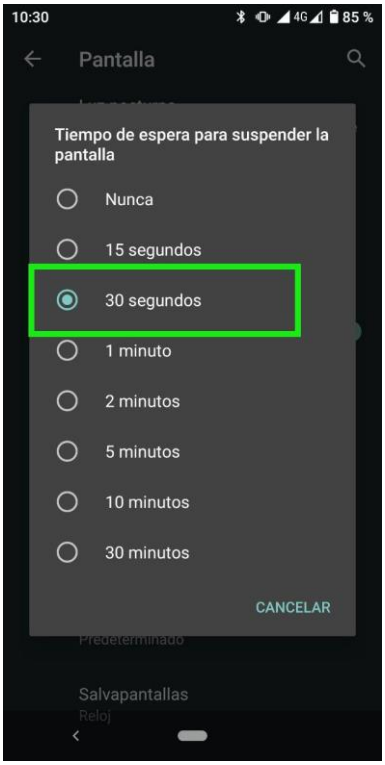


  Con todo, cada vez que queramos usar el móvil, nos solicitará el pin, contraseña, patrón o huella definido para su desbloqueo.
  Por último, cabe destacar algo muy importante en cuanto a la pantalla (no ya sobre la seguridad en sí pero sí como complemento). Entre las opciones de la sección de "Ajustes del dispositivo", está la categoría de "Pantalla":

En esta categoría de “Ajustes de Pantalla”, en el caso del Xiaomi MI A2 utilizado en estos ejemplos, accediendo a opciones avanzadas se puede seleccionar el “Tiempo de espera para suspender la pantalla”:



Esta opción nos permite programar el dispositivo para que, por ejemplo, tras 15 segundos sin que se haya usado, 30 segundos, 1 minuto, etc., se bloquee y no pueda usarse sin desbloquearlo con la opción que hayamos marcado en la seguridad (patrón, PIN, contraseña, o la huella digital, etc.). En el caso del ejemplo siguiente se delimita a 30 segundos. Quiere decir que tras 30 segundos sin usar el teléfono, se bloquearía y solo podremos usarlo tras desbloquearlo. Es una gran medida de seguridad ya que permite bloquear el móvil para mayor seguridad de forma automática tras un cierto intervalo de tiempo:



Siguiendo todos los pasos hasta aquí explicados, garantizamos que nadie pueda acceder a nuestro móvil y los datos en caso de pérdida o robo. Habremos perdido o nos habrán robado el móvil, pero nuestros datos e información tendrán un extra de seguridad y privacidad gracias al sistema de bloqueo. Si no conocen el PIN, patrón, contraseña, y menos aún si no tienen nuestra huella digital, no podrán acceder como tal al contenido del móvil.

Por si alguna vez perdemos o nos roban el móvil con Android, es interesante la información de la sección de la ayuda de Android sobre "Encontrar tu dispositivo Android"

2.2. Dispositivo iOS

En el caso de los dispositivos con iOS, la misma página del Manual de uso del iPhone aconseja lo siguiente para proteger el acceso al iPhone (cabe recordar que se añade la información del sistema iOS 16, pero que en la misma página se puede seleccionar la opción de iOS 14 e iOS 15):

- **Definir un código seguro**: el procedimiento es muy similar al visto para un dispositivo Android aunque con algunas particularidades en la terminología empleada. En esta página, el Manual del iPhone da las instrucciones precisas para: definir o cambiar el código, cambiar cuándo se bloquea el iPhone automáticamente, borrar datos después de 10 códigos fallidos, desactivar el código, y restablecer el código.
- **Usar Face ID o Touch ID**: esta opción depende del modelo de iPhone que tengas. Puedes consultar los modelos compatibles con Face ID desde aquí, y con Touch ID desde aquí. Es un extra que proporciona una forma segura y cómoda para desbloquear el iPhone, y para autorizar compras y pagos e iniciar sesión en muchas apps de terceros. Aquí tienes información ampliada para configurar el Face ID en el iPhone o el Touch ID en el iPhone.
- iOS nos da también la posibilidad de controlar qué funciones estarían disponibles sin desbloquear el iPhone. En esta web hay información práctica sobre cómo permitir o denegar el acceso a algunas funciones cuando el dispositivo está bloqueado.
- Como en el caso de Android, iPhone también dispone de una web para Buscar tu iPhone en caso de pérdida o robo.

3. Contraseñas y Seguridad a nivel de apps en el Smartphone

3.1. Para Android

Los dispositivos Android son sistemas en los que ejecutamos diferentes aplicaciones o apps, siendo necesario el uso de contraseñas para multitud de servicios y plataformas como redes sociales y un largo etcétera. Un buen uso, elección y una buena gestión de las contraseñas es esencial para ganar en seguridad.

Para quienes utilicen Android hay algunos aspectos a considerar:

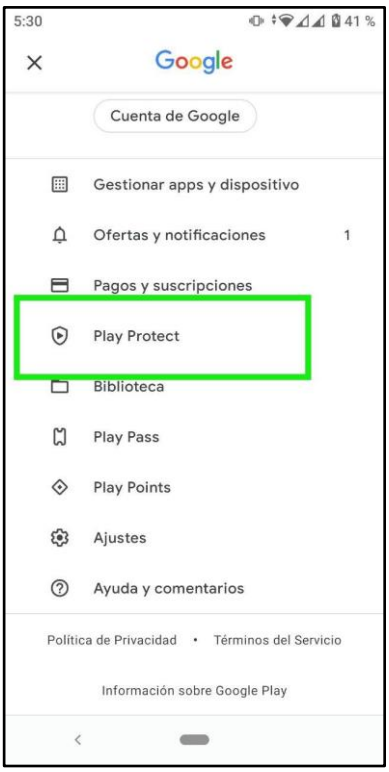
- La posibilidad de usar Google Play para proteger las aplicaciones y la privacidad de nuestros datos
- Generar contraseñas seguras

Usando Google Play Protect para proteger nuestras aplicaciones y la privacidad de nuestros datos

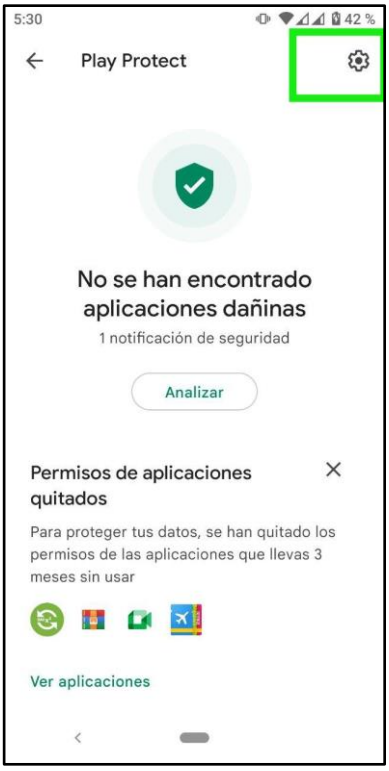
Es importante saber que Google Play Protect está activado de forma predeterminada. La misma Ayuda de Android de Google tiene una sección para el uso de Google Play Protect. Para usarlo, habría que seguir estos pasos:

- Abrimos la aplicación “Google Play Store” y arriba a la derecha, accedemos al icono de perfil (en la captura aparece un cuadrado con el borde verde y dentro un círculo negro como foto o icono de perfil).

- Accedemos a “Play Protect Ajustes”



- Una vez dentro, pulsamos en el icono de configuración u opciones:



- Activamos la opción “Analizar aplicaciones con Play Protect” y todas las que haya:

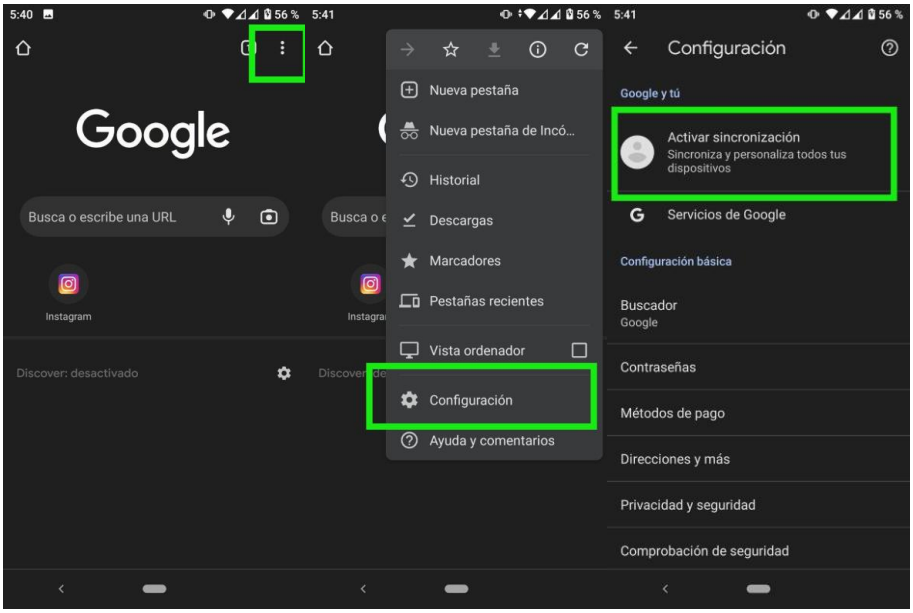
Con Google Play Protect podemos conseguir lo siguiente:

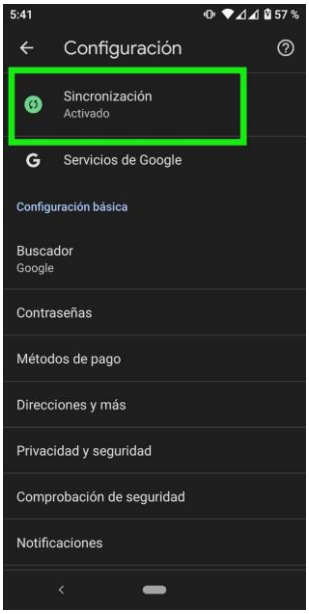
- Google Play Protect comprueba si hay comportamientos dañinos en nuestras aplicaciones y dispositivos.
- Comprueba la seguridad de las aplicaciones de Google Play Store antes de que las descarguemos.
- Analiza nuestro dispositivo en busca de aplicaciones potencialmente dañinas que provengan de otras fuentes. Estas aplicaciones dañinas pueden ser software malicioso.
- Nos advierte de aplicaciones potencialmente dañinas.
- Puede desactivar las aplicaciones dañinas o quitarlas del dispositivo.
- Nos advierte si detecta aplicaciones que infringen nuestra Política de Software No Deseado porque ocultan o falsean información importante.
- Nos envía alertas de privacidad sobre las aplicaciones que pueden obtener permisos de usuario para acceder a tu información personal, lo que infringe su Política para Desarrolladores.
- También puede restablecer los permisos de las aplicaciones para proteger nuestra privacidad en determinadas versiones de Android.

Gestión de contraseñas en Google Chrome

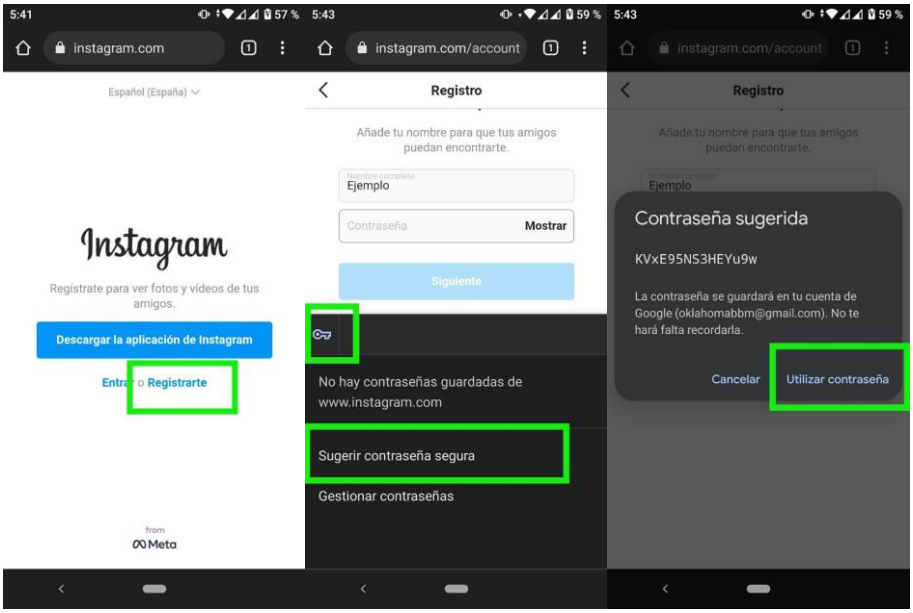
Si usamos un sistema Android, que es de Google, muy probablemente usamos también el navegador Google Chrome para Internet. Si usamos Chrome, nos da la posibilidad de una buena sincronización e incluso dispone de una opción que nos permite generar una contraseña segura. Todo esto lo podemos encontrar en la página de la Ayuda de Android de Google "Generando contraseñas seguras". Para generar contraseñas seguras tenemos que hacer lo siguiente:

1. Activar la sincronización en Chrome:



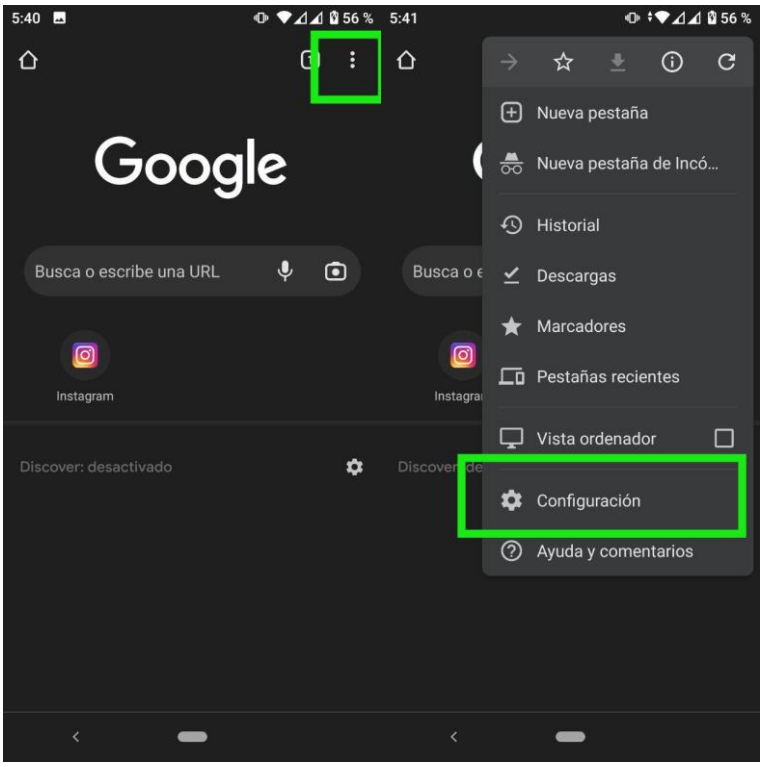


2. Una vez activada la sincronización, si vamos a un sitio web y nos tenemos que registrar para abrir o crear una cuenta en el servicio o plataforma que queramos, al tocar el cuadro de texto de la contraseña a introducir, Google Chrome nos sugerirá una contraseña segura (veremos un símbolo similar a una llave que hemos de pulsar; y nos sale la opción de “sugerir contraseña segura”, que si seleccionamos, nos ofrece una contraseña segura). Para confirmarla, seleccionaremos la opción de ”Utilizar contraseña”.

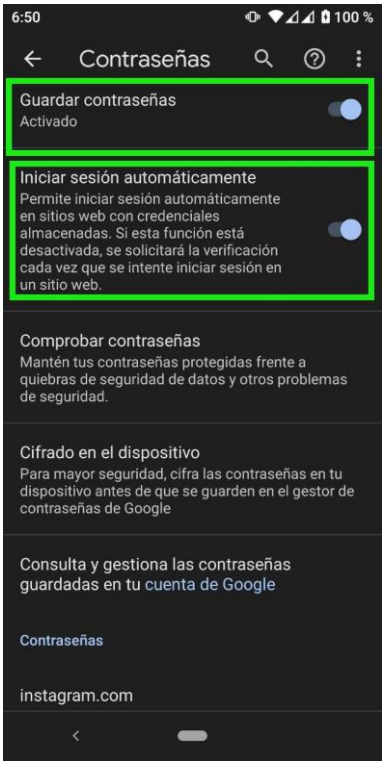


3. Cuando terminemos de registrarnos para crear la cuenta, la contraseña se guardará automáticamente en Chrome.

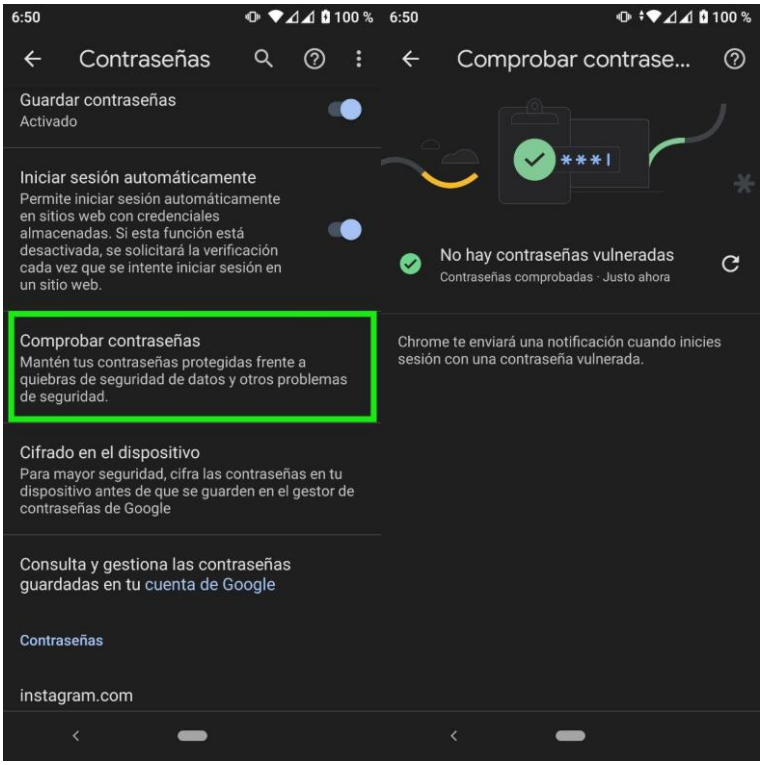
Una vez creadas las contraseñas seguras con Google Chrome, el navegador permite realizar una serie de opciones para ganar en seguridad y privacidad. Para ello hay que acceder a la sección de configuración en Chrome; y una vez ahí a la de contraseñas:



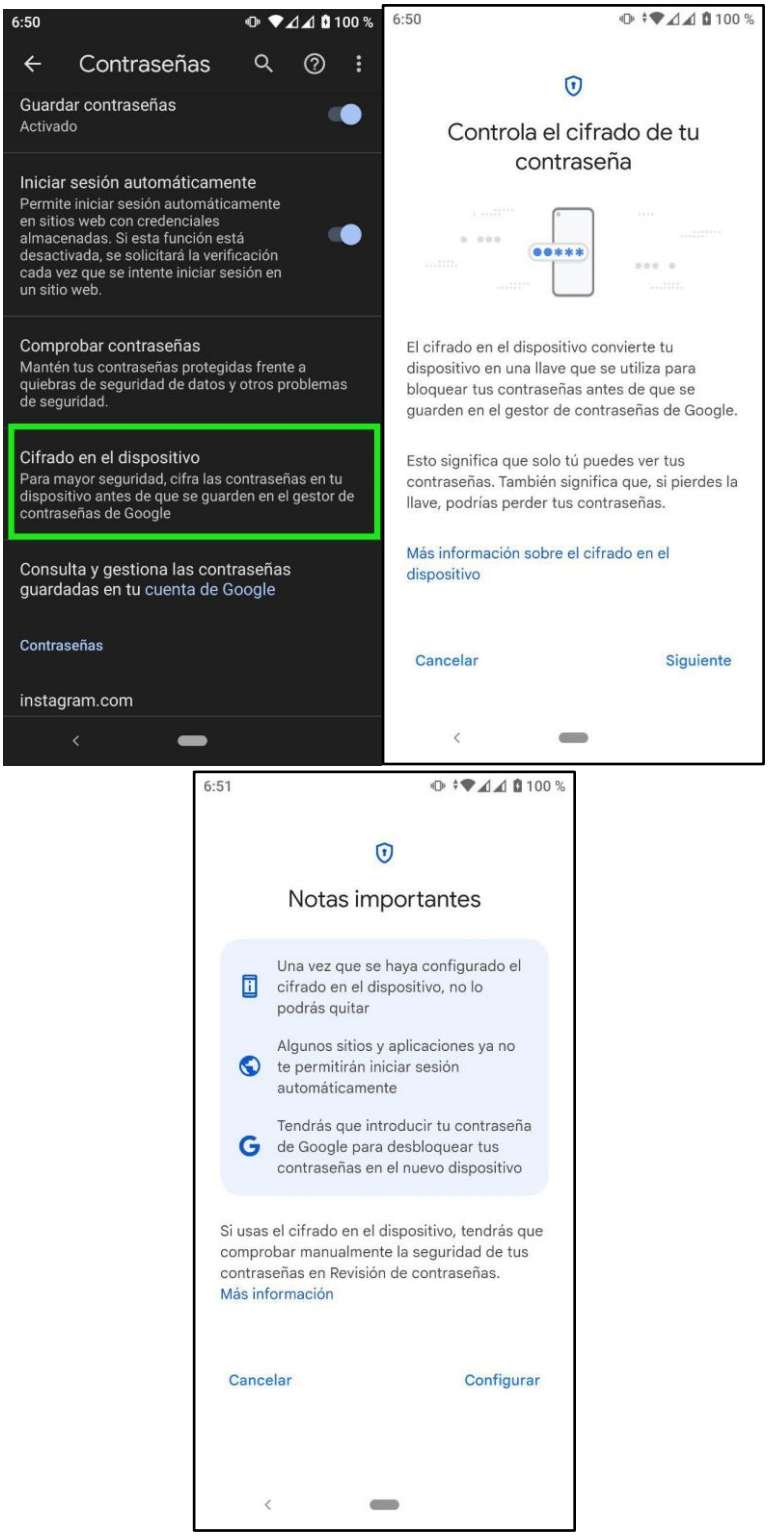
En primer lugar, podemos decidir si queremos guardar las contraseñas o no, y si queremos iniciar sesión automáticamente en los servicios en que hayamos grabado o guardado la contraseña. Lo más seguro sería tener que poner las contraseñas cada vez y ni siquiera tenerlas guardadas. Pero la realidad es que hay que buscar un equilibrio entre lo seguro y lo cómodo (sería muy difícil recordar todas las contraseñas, y más aún si las hemos creado con las sugerencias seguras de Chrome):



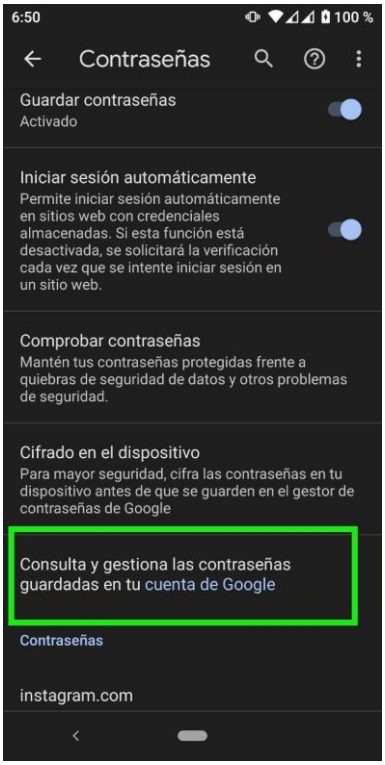
También nos ofrecen la posibilidad de comprobar contraseñas. Esta opción permite comprobar si alguna de nuestras contraseñas ha sido vulnerada. Es una protección extra que conviene revisar de vez en cuando, aunque Google nos avisará igualmente si una de nuestras contraseñas ha sido vulnerada:



Otra de las opciones es la de “Cifrado en el dispositivo”. Es también un extra de seguridad que permite cifrar las contraseñas en el dispositivo (en el móvil) antes de que se guarden en el gestor de contraseñas de Google. Digamos que el cifrado en el dispositivo convierte nuestros móviles en una llave para bloquear las contraseñas, lo que significa que solo nosotros podremos ver nuestras contraseñas. Pero tiene un riesgo, y es que si perdemos esa llave generada para cifrar, podríamos perder todas nuestras contraseñas. Por ello hay que pensar bien si queremos esta opción:

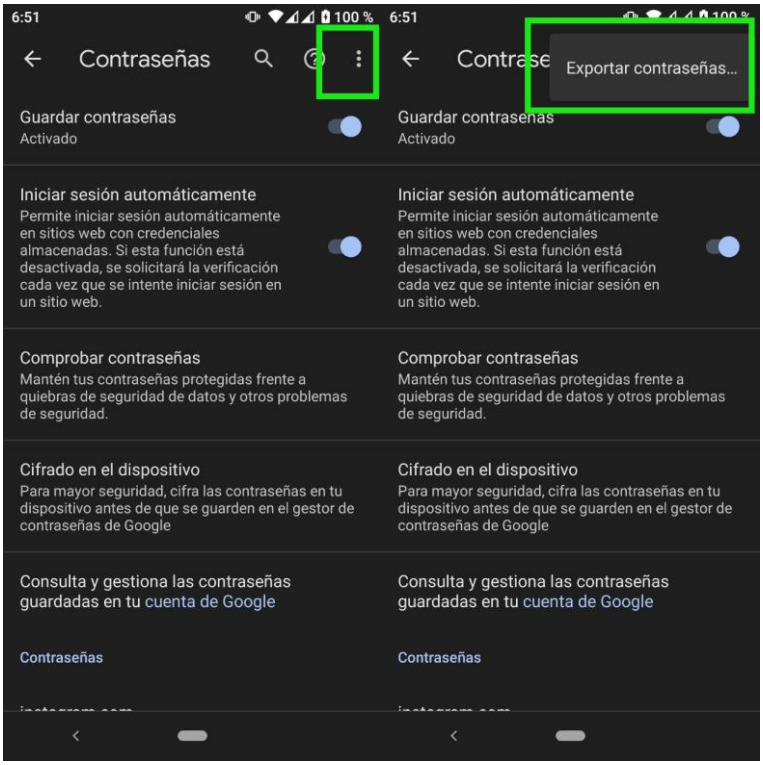


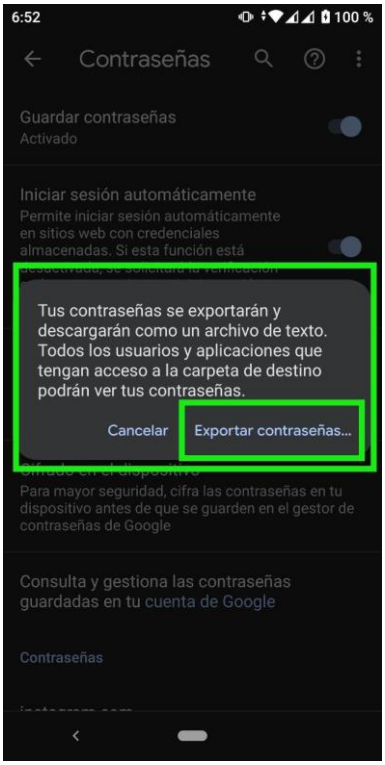
Tenemos la opción de consultar y gestionar las contraseñas guardadas en la cuenta de Google desde la siguiente opción:



Si accedemos a dicha opción, veremos el gestor de contraseñas desde donde también podemos revisarlas y consultarlas, cambiarlas o quitarlas:

Por último, podemos exportar las contraseñas y descargarlas en caso de que queramos hacer una copia de seguridad de las mismas. Desde el inicio de la sección de Contraseñas en Chrome, hemos de seleccionar los 3 puntos verticales de la esquina superior derecha:





El canal de Google España en Youtube dispone de algunos vídeos interesantes sobre la seguridad y las contraseñas:

- Revisión de contraseñas
- La manera más segura de recordar tu contraseña
- Una forma más segura de gestionar tus contraseñas

Por último, para quien use Firefox, tal vez le interese la sección de la ayuda de Firefox dedicada a guardar contraseñas Contraseñas y la de administrarlas.

3.2. Para iOS

La ayuda de iOS para los iPhones incluye información sobre cómo hacer que los inicios en cuentas sean más sencillo y más seguros. Toda esta información está extraída de esta página del manual de iOS para el iPhone. Estas son las opciones:

- *Iniciar sesión con llaves de acceso:* Las llaves de acceso nos permiten iniciar sesión en cuentas de sitios web y apps con Face ID o Touch ID en lugar de una contraseña. Como una llave de acceso no sale de los dispositivos en los que has iniciado sesión con el ID de Apple, y dado que es específica del sitio web o app para el que se crea, está protegida frente a fugas e intentos de suplantación de identidad. A diferencia de una contraseña, no tenemos que crear, proteger ni recordar una llave de acceso.
- *Usar "Iniciar sesión con Apple":* Podemos usar nuestro ID de Apple en lugar de crear y recordar nombres de usuario y contraseñas para iniciar sesión en cuentas. "Iniciar sesión con Apple" también proporciona la seguridad de la autenticación de doble factor y limita la información compartida sobre nosotros.
- *Dejar que el iPhone cree contraseñas seguras:* Si nos registramos en un servicio que no admite llaves de acceso ni "Iniciar sesión con Apple", deja que el iPhone cree automáticamente una contraseña segura que no tendrás que memorizar.
  También, iOS ofrece información sobre otras formas de hacer que el inicio de sesión sea más seguro y sencillo con todas nuestras contraseñas de sitios web y apps.
- *Reemplazar contraseñas débiles:* Si creamos contraseñas débiles o filtradas, el iPhone las identifica automáticamente para que las cambiemos.
- *Compartir llaves de acceso y contraseñas de forma segura.* Podemos usar AirDrop para compartir de forma segura una llave de acceso o una contraseña con otra persona que use un iPhone, iPad o Mac.
- *Utilizar el sistema de autenticación integrado para la autenticación de doble factor:* Para los sitios web y apps que ofrecen autenticación de doble factor, podemos rellenar con códigos de verificación generados automáticamente sin tener que basarnos en códigos SMS o en otras apps.
- *Rellenar fácilmente códigos en formato SMS:* Podemos rellenar códigos de un solo uso automáticamente enviados desde sitios web o apps al iPhone.
- *Mantener actualizadas las llaves de acceso y contraseñas en todos tus dispositivos:* El llavero de iCloud mantiene tus credenciales actualizadas automáticamente en todos nuestros otros dispositivos.
  El manual de iOS también ofrece indicaciones sobre cómo:

- Gestionar la información que se comparte con otras personas y con las apps
- Proteger la privacidad de los correos electrónicos
- Proteger la navegación web
- Aislar el iPhone cuando se enfrenta a un ciberataque sofisticado

Todo ello se puede consultar en la sección dedicada a usar las medidas de seguridad y protección de la privacidad integradas del iPhone.

4. Para acabar: software para la gestión y creación seguras de contraseñas

En este documento se han explicado procedimientos para mejorar la seguridad en dispositivos Android e iOS. Se ha centrado la atención y explicación en el navegador Google Chrome asumiendo que puede ser el más usado en dispositivos Android. También, se han añadido algunas referencias para quien use el navegador Firefox. La realidad es que las explicaciones sobre seguridad en los dispositivos móviles dependen en parte de qué marca, modelo y versión del sistema operativo que se use. Por eso, esta guía tiene la limitación de haberse centrado especialmente en Android y Google Chrome, con contenidos para sistemas o dispositivos iOS (iPhones) y también en navegadores como Firefox.

En el ámbito de la seguridad y gestión de contraseñas a nivel de dispositivos móviles y de escritorio (ordenadores personales o portátiles), el software para la gestión de contraseñas también es muy útil. En ese sentido, cabe resaltar software como Keepass, software libre y multiplataforma disponible para sistemas con Android, iPhone, Linux, Windows y MacOS y como extensión en navegadores como Firefox y Chrome entre muchos otros. En la misma web de Keepass podemos leer en qué consiste este software:

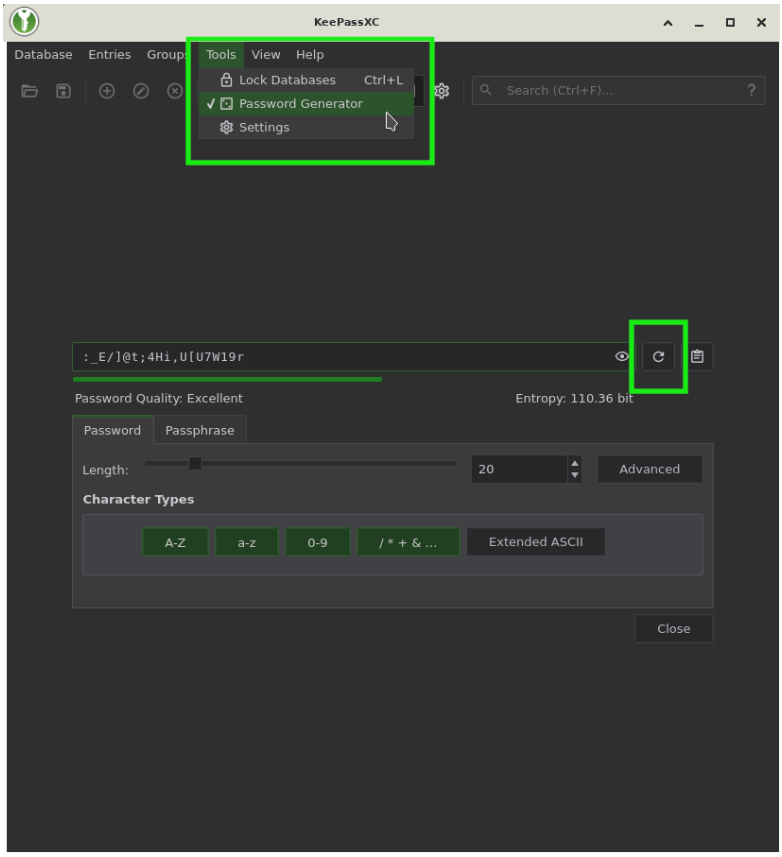
“Hoy en día, tenemos que recordar muchas contraseñas. Necesitamos una contraseña para muchos sitios web, nuestra cuenta de correo electrónico, los inicios de sesión en la red, etc. La lista es interminable. Además, deberíamos usar una contraseña diferente para cada cuenta, porque si usáramos una sola contraseña en todas partes y alguien consiguiera esta contraseña, tendríamos un problema: esa persona tendría acceso a todas nuestras cuentas”.

Y añaden que:

“KeePass es un gestor de contraseñas libre, gratuito y de código abierto, que nos ayuda a gestionar nuestras contraseñas de forma segura. Podemos almacenar todas tus contraseñas en una base de datos, que se bloquea con una llave maestra. Así que sólo tenemos que recordar una única llave maestra para desbloquear toda la base de datos. Los archivos de la base de datos se encriptan utilizando los mejores y más seguros algoritmos de encriptación conocidos actualmente (AES-256, ChaCha20 y Twofish)”.

Una de las opciones que ofrece Keepass, además de ser un gestor seguro de contraseñas que podemos sincronizar en los móviles, ordenadores y diferentes sistemas operativos, es su herramienta de generación de contraseñas seguras (en la siguiente captura, se puede acceder a dicha opción desde la pestaña de “Tools”, señalada en verde). Por defecto, nos crea una contraseña de excelente calidad en cuanto a seguridad. Incluso podemos seleccionar la longitud que queremos para

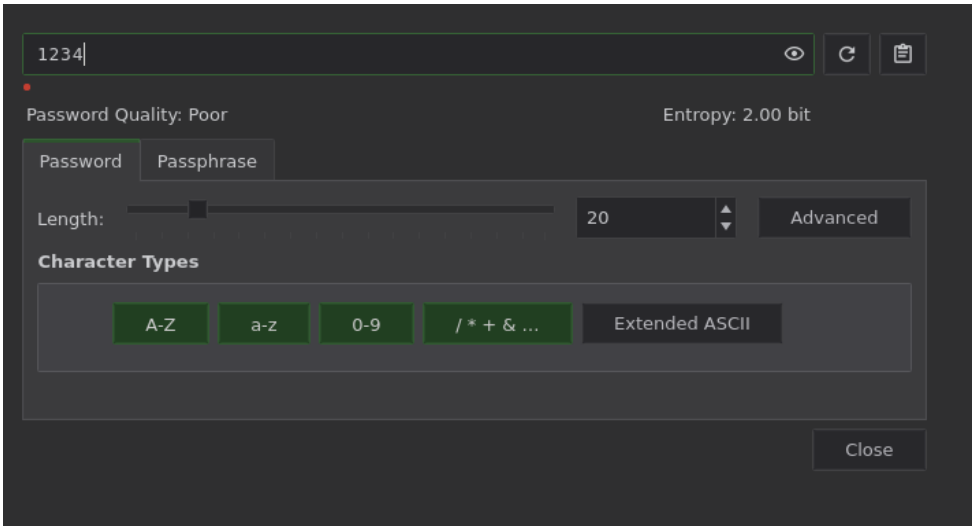
nuestra nueva contraseña y qué tipo de caracteres incluir. Podemos crear diferentes contraseñas de calidad excelente con el botón de renovar señalado en verde en la siguiente captura:

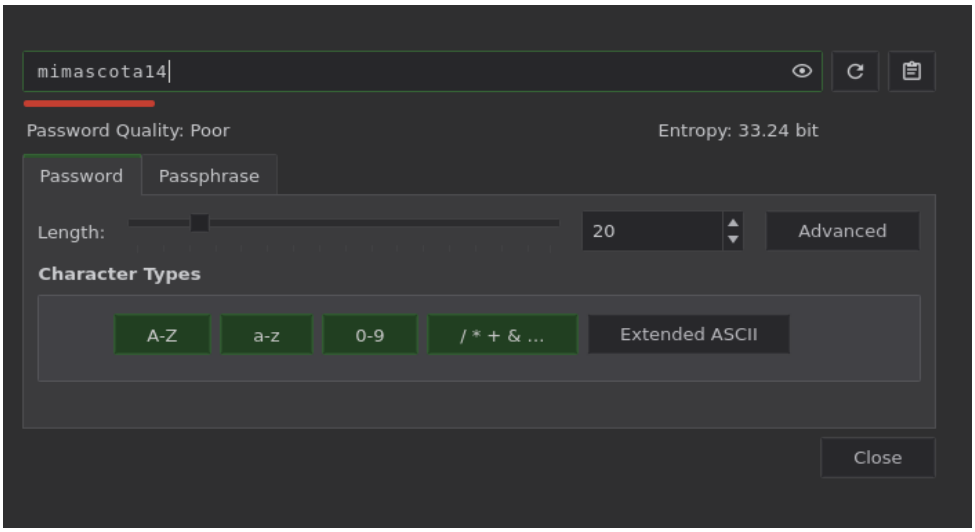


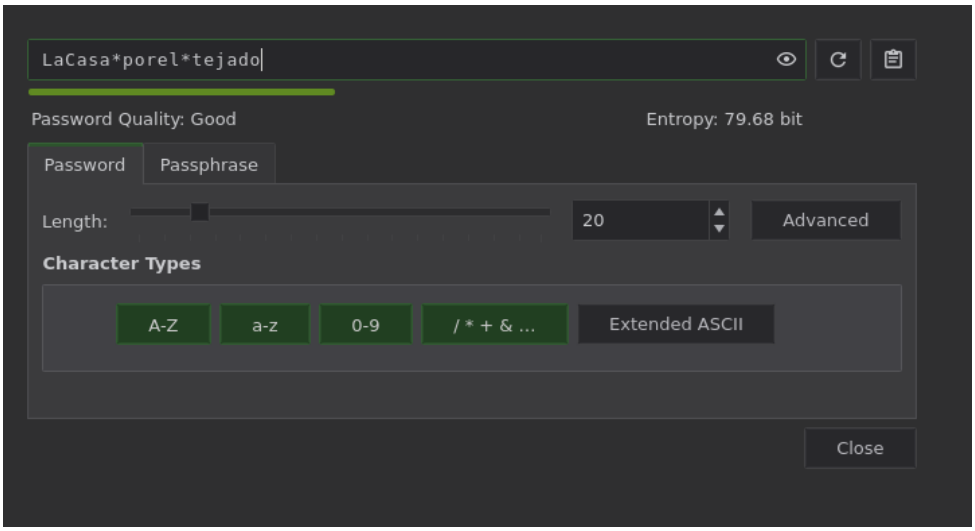
En la captura anterior, la contraseña segura de 20 dígitos que nos ha creado Keepass es la de:

- :_E/]@t;4Hi,U[U7W19r

Pero si queremos escribir una contraseña de manera propia, el mismo software nos ofrece información sobre su grado de seguridad. En las siguientes capturas se puede ver que la contraseña *1234* es pésima en cuanto a calidad y seguridad (nos lo dice el resultado de “Password Quality: Poor”); *mimascota14* es igualmente desaconsejable aunque mejor que la de *1234*; y que una contraseña del tipo *LaCasa*porel*tejado*, que mezcla mayúsculas con símbolos como el asterisco, resulta de buena calidad (ya con la barra verde en lugar de la roja simbolizando su calidad). No obstante, ninguna llega a la calidad tan alta de la generada por Keepass de la captura anterior:







Por todo ello, Keepass es una gran herramienta no solo para guardar y gestionar contraseñas, sino también para crearlas, aconsejando utilizar las que ofrece el mismo software por su alta calidad para la seguridad. Keepass se puede descargar desde la sección de Descargas de su página web.

Recursos utilizados

Aunque se han nombrado en el documento, para la redacción de todo el contenido se han utilizado las fuentes oficiales de manuales y ayuda de Google para Android y Chrome, y de iOS para los dispositivos iPhone. No obstante, se resaltan aquí los recursos principales utilizados:

- Ayuda de Android
- Manual de uso del iPhone
- Configurar el bloqueo de pantalla en dispositivos Android
- Usar Google Play Protect para proteger tus aplicaciones y la privacidad de tus datos
- Generar una contraseña (Ayuda de Google Chrome)
- Canal de Google España en Youtube
- KeePass Password Safe

Para repasar: 6 preguntas y 1 caso práctico

6 preguntas

Esta actividad consiste en seleccionar la opción que te parezca correcta y en explicar el motivo para las siguientes situaciones

1. **Para ganar en seguridad en nuestro Smartphone, tenemos la opción de deslizar la pantalla**:

a. Correcto, la opción de deslizar es la que más seguridad otorga
b. Incorrecto, esta opción no aporta ningún tipo de seguridad

Motivo:

2. **Las opciones de bloqueo de pantalla de nuestro smartphone son:**

a. Patrón, que consiste en diseñar una traza que habremos de indicar al Smartphone para poder desbloquearlo y usarlo
b. PIN: consiste en un número de al menos 4 dígitos
c. Contraseña: consiste en un conjunto de valores alfanuméricos, esto es, que puede contener números y letras
d. En algunos smartphones también existe la posibilidad de utilizar la huella dactilar
e. Todas son correctas

Motivo:

3. **¿Se pueden tomar más medidas para mejorar la seguridad de nuestro Smartphone?**

a. No, solo podemos usar la opción de bloqueo de la pantalla
b. Sí, es aconsejable definir un tiempo en segundos o minutos para que la pantalla del smartphone se bloquee automáticamente tras cumplirse dicho tiempo

Motivo:

4. **¿Cuál de las siguientes contraseñas para acceder a cualquier red social o plataforma desde un navegador web te parece más segura?**

a. 1234
b. 5555
c. MiMascotaJimmy

Motivo:

5. **¿Cuál de las siguientes contraseñas para acceder a cualquier red social o plataforma desde un navegador web te parece más segura?**

a. MiMascotaJimmy
b. Mi*Mascota*Jimmy

Motivo:

6. **¿Cuál de las siguientes contraseñas para acceder a cualquier red social o plataforma desde un navegador web te parece más segura?**

a. M1*M4scot4*Ji88y
b. $Nt|IQ::6N48i$PY\l.*

Motivo:

Caso práctico

- Elige uno de los sistemas de bloqueo de pantalla que hemos visto (patrón, PIN, contraseña) y procede a añadirlo a tu Smartphone. Este caso práctico consiste en que expliques cómo lo has hecho hasta conseguirlo. Puedes hacerlo por pasos. Es como si tuvieras que explicar a una persona que no conoce las opciones de bloqueo de pantalla en el Smartphone cómo hacerlo. Dicho de otra forma, ahora eres tu la experta o el experto y le vas a enseñar a alguien cómo conseguirlo.