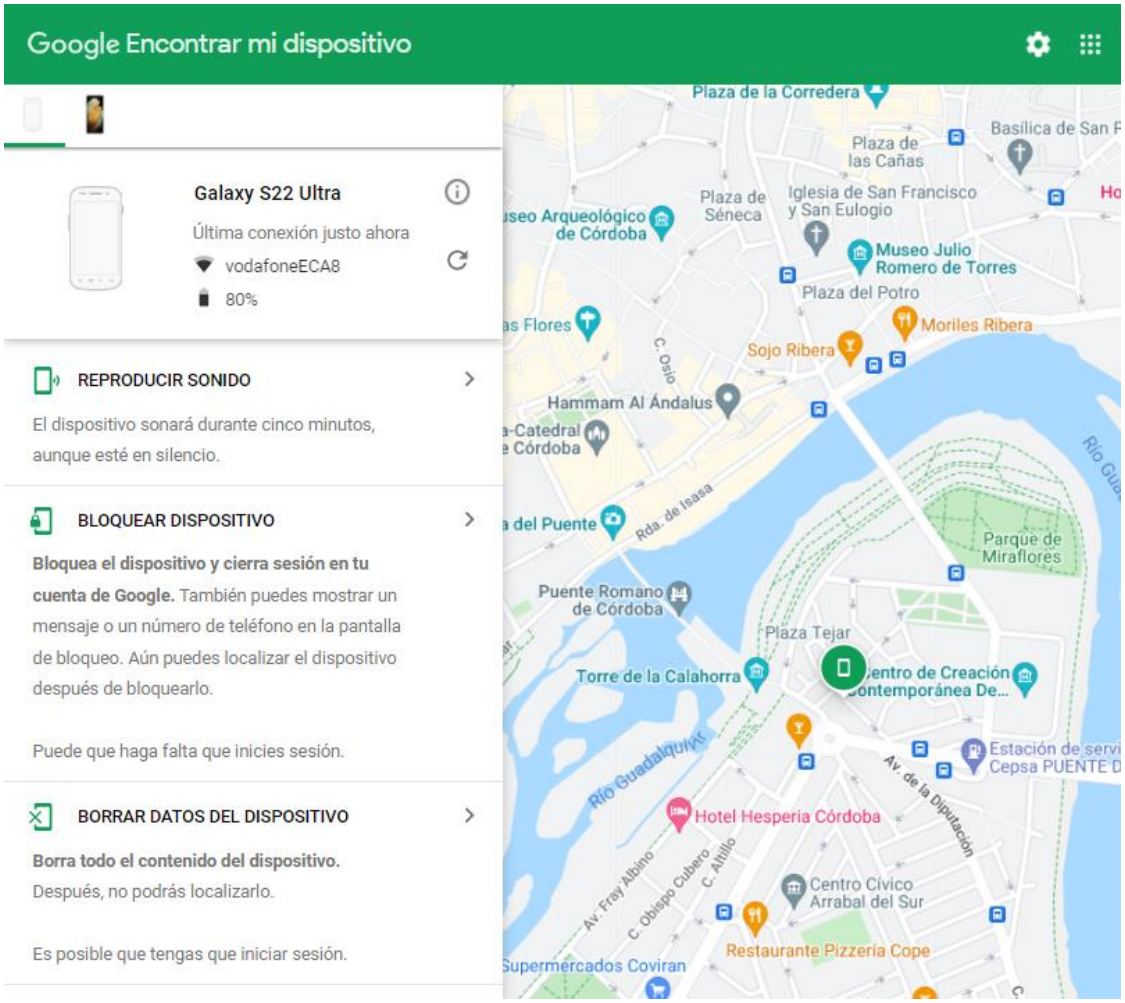
RESUMEN FINAL DEL CURSO: PUNTOS MÁS RELEVANTES

Hemos llegado al final de nuestro curso de "Seguridad en dispositivos móviles Android", en el que hemos aprendido todo lo relacionado con la seguridad en nuestros dispositivos y las principales amenazas a las que estamos expuestos, así como las mejores prácticas para asegurar que mantenemos nuestra información a buen recaudo.

En este resumen final, haremos un repaso general sobre los principales conceptos y conocimientos que hemos adquirido a lo largo del curso.

Una de las primeras medidas que aprendimos para proteger nuestro dispositivo es el **bloqueo de acceso al dispositivo**, mediante patrón, PIN, contraseña o biometría.

Además, el concepto de **autenticación en dos pasos** es muy importante para acceder a nuestras cuentas, y nos dará un extra de seguridad muy interesante para proteger la **cuenta de Google de acceso no deseados**. Google, además, pone a nuestra disposición en Android la funcionalidad de **Encontrar mi móvil** (*Find my device*), que nos ayudará a rastrearlo y localizarlo en caso de robo o pérdida. De manera adicional, esta funcionalidad nos permitirá hacer un **borrado remoto** de datos para proteger nuestra confidencialidad en caso de que no podamos recuperarlo.



Android también pone a nuestra disposición una funcionalidad algo extrema en caso de que necesitemos eliminar por completo toda la información y configuraciones almacenadas en nuestro dispositivo**.** El conocido como **"*hard-reset*" o restauración a valores de fábrica,** que sirve para dejar el dispositivo como el primer día de manera segura, ayudando a una rápida desvinculación de todas tus cuentas y eliminación de datos en el dispositivo.

Ya que nuestros dispositivos se han convertido en un auténtico almacén de datos, son muy importantes tanto el conocimiento y protección de los **modos de almacenamiento** (interno, externo y en la nube) como el **cifrado de la información** para evitar que sea legible en caso de fuga de datos. Además, conocer cómo realizar **copias de seguridad** y **restaurar la información** almacenada en nuestros dispositivos hará que podamos estar tranquilos en caso de avería, pérdida y robo, ya que todos nuestros datos podrán ser volcados a un nuevo dispositivo de manera sencilla.

Por supuesto no podemos olvidar que gran parte de esta información, especialmente aquella almacenada en la nube o en aplicaciones, está protegida mediante contraseña de acceso a nuestra cuenta de usuario, para lo que es importante usar contraseñas robustas, y muy recomendable el uso de un **gestor de contraseñas**, que nos ayudará a crear y guardar contraseñas únicas y seguras para no tener que recordarlas o anotarlas en algún lugar que pueda generar riesgos.

Como mencionábamos anteriormente, la gran cantidad de información que almacenamos en nuestros dispositivos hace que los ciberdelincuentes usen diferentes técnicas para intentar conseguir acceso a esta información para fines maliciosos.

Uno de los principales modos usados es mediante la infección por ***malware*****,** un *software* malicioso más conocido como virus que también existe en Android e intentará apoderarse de tu dispositivo, contraseñas e información personal. Aunque existen muchas subcategorías, podemos destacar cinco tipos principales de *malware*:

1. **El *ransomware***, que cifra todos o parte de nuestros archivos, haciéndolos inaccesibles, y nos pide un pago de un rescate (*ransom* en inglés) para volver a tener acceso a nuestra información.

2. **El *spyware***, un tipo muy común y que se caracteriza por trabajar en silencio, recopilando datos del usuario, navegación, contraseñas e incluso información bancaria o métodos de pago.

3. **Los gusanos**, cuyo objetivo principal es extenderse e infectar en mayor número de dispositivos posibles, en ocasiones para instalar algún tipo de *malware*.

4. **El *adware*,** que se centra en generar beneficios para el atacante a través de anuncios no deseados que se muestran en el dispositivo infectado.

5. **Los troyanos,** cuya principal característica es su capacidad para pasar totalmente inadvertidos hasta que llega el momento de efectuar las tareas maliciosas para las que están programados.

Para combatir el *malware* es importante el uso de antivirus (***Anti-malware***), contralar las potenciales vías de infección y, como método preventivo, **mantener actualizados** tanto el sistema Android como las aplicaciones que instalamos en el dispositivo.

Otro método muy usado por ciberdelincuentes es la **ingeniería social**, una práctica para obtener información confidencial a través de la manipulación de usuarios, y que está en auge como herramienta para obtener información, acceso o permisos en nuestros dispositivos. Identificar el engaño a tiempo, no compartir información confidencial ni descargar archivos o programas es la mejor y única forma de combatirla.

Por otro lado, hemos conocido en profundidad algunas de las características más importantes en cuanto a conectividad de los dispositivos Android. Las **redes Wi-Fi** y cómo usarlas de manera segura, dado lo extendido de su uso, es un punto importantísimo para mantener nuestros

dispositivos y su información a salvo, por lo que conectar a redes seguras nos ayudará a proteger la información que transmitimos, así como configurar contraseñas robustas y seleccionar un cifrado fuerte en nuestra red doméstica. De igual forma, el archiconocido sistema ***Bluetooth*** nos ayuda a emparejar nuestro dispositivo con diferentes periféricos como auriculares, altavoces o relojes inteligentes, pero también abre una posibilidad de acceso a nuestro dispositivo, que ha de cerrarse mediante el uso de configuraciones seguras y códigos de verificación.

Otro de los aspectos de conectividad más importantes es el relacionado con el GPS y la **geolocalización** de nuestros dispositivos, que nos permite conocer donde se encuentra un dispositivo, compartir nuestra ubicación u obtener resultados de búsquedas basados en nuestro entorno. Administrar correctamente esta funcionalidad es crucial para mantener nuestra privacidad y seguridad a salvo, y la premisa es clara: restringir el acceso a la ubicación solo a aquellas aplicaciones que realmente lo necesiten y sólo cuando lo necesiten.

Adicionalmente, la tecnología **NFC (*Near Field Communication*)** nos permite principalmente realizar pagos a través de nuestro dispositivo, con un radio de acción muy bajo, al estilo de una tarjeta de crédito *contactless*, además de la transferencia de archivos y otras tareas. Hay que asegurar que solo nosotros decidimos cuándo y cómo nuestro dispositivo usa esta tecnología para así evitar sorpresas indeseadas.

Haciendo uso del sistema NFC, hemos aprendido el funcionamiento de **Google Pay,** uno de los sistemas de pago móvil más utilizados por su facilidad de uso, pero también por su seguridad, ya que sus características hacen de él una herramienta perfecta para realizar pagos tanto de manera presencial como online evitando ser víctimas de fraudes.

Muy relevante también es el uso e instalación de **aplicaciones**, ya que estos procesos abren una puerta de acceso a nuestro dispositivo, por lo que es importante asegurar la descarga de aplicaciones de tiendas o repositorios de confianza y gestionar los **permisos** que solicitan, de manera que solo aquellos necesarios para su funcionamiento sean activados en la app.

Dentro de las aplicaciones, además, hemos recomendado algunas en diferentes ámbitos de la seguridad que pueden sernos de mucha utilidad, como es el caso de aplicaciones:

1. **Antirrobo:** para poder reaccionar en caso de robo o pérdida de nuestros dispositivos.
2. **Cortafuegos:** para bloquear intentos de acceso no autorizados.
3. **Antivirus:** para prevenir y detectar infecciones de *malware.*
4. **Análisis de tráfico:** para entender qué estamos recibiendo o enviando y a dónde, durante nuestras conexiones a Internet.

Con este pequeño resumen de todo lo que hemos aprendido a lo largo del curso de “Seguridad para dispositivos Android” terminamos, esperando que hayáis disfrutado y aprendido todo lo necesario para proteger los dispositivos Android, la información que almacenan y a sacar partido a todas sus funcionalidades de una forma segura.

¡Muchas gracias y hasta pronto!