

Taller formativo

Seguridad en dispositivos Android e iOS

LICENCIA DE CONTENIDOS

La presente publicación pertenece a Instituto Nacional de Ciberseguridad (INCIBE) y está bajo licencia Reconocimiento-No Comercial-CompartirIgual 4.0 Internacional de Creative Commons. Por esta razón está permitido copiar, distribuir y comunicar públicamente esta obra bajo las condiciones siguientes:

- **Reconocimiento.** El contenido de esta publicación se puede reproducir total o parcialmente por terceros, citando su procedencia y haciendo referencia expresa a INCIBE y su sitio web: <https://www.incibe.es>. Dicho reconocimiento no podrá en ningún caso sugerir que INCIBE presta apoyo a dicho tercero o apoya el uso que hace de su obra.
- **Uso No Comercial.** El material original y los trabajos derivados pueden ser distribuidos, copiados y exhibidos mientras su uso no tenga fines comerciales.
- **Compartir Igual.** Si altera o transforma esta obra, o genera una obra derivada, sólo puede distribuirla bajo esta misma licencia.

Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra.

Alguna de estas condiciones puede no aplicarse si se obtiene el permiso de INCIBE como titular de los derechos de autor.

Texto completo de la licencia:

https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es_ES



ÍNDICE

1. Objeto del documento.....	5
2. Organización y estructura	6
3. Objetivo	7
4. Metodología y recursos	8
5. Contenidos.....	9
5.1. Diapositiva 1. Presentación del taller	9
5.2. Diapositiva 2. Índice	9
5.3. Diapositiva 3. Introducción	9
5.4. Diapositiva 4. Bloqueo de pantalla	9
5.5. Diapositiva 5. Bloqueo de pantalla	10
5.6. Diapositiva 6. Actividad 1	10
5.7. Diapositiva 7. Actualizaciones automáticas	10
5.8. Diapositiva 8. Actualizaciones automáticas	11
5.9. Diapositiva 9. Actividad 2	11
5.10. Diapositiva 10. Software de seguridad.....	11
5.11. Diapositiva 11. Software de seguridad.....	12
5.12. Diapositiva 12. Software de seguridad.....	12
5.13. Diapositiva 13. Software de seguridad.....	12
5.14. Diapositiva 14. Copias de seguridad.....	13
5.15. Diapositiva 15. Copias de seguridad.....	13
5.16. Diapositiva 16. Actividad 3	13
5.17. Diapositiva 17. Redes inalámbricas del dispositivo.....	14
5.18. Diapositiva 18. Redes inalámbricas del dispositivo: Bluetooth.....	14
5.19. Diapositiva 19. Redes inalámbricas del dispositivo: wifi.....	14
5.20. Diapositiva 20. Redes inalámbricas del dispositivo: VPN	15
5.21. Diapositiva 21. Redes inalámbricas del dispositivo: NFC	15
5.22. Diapositiva 22. Descarga de aplicaciones desde un sitio seguro.....	15
5.23. Diapositiva 23. Permisos de aplicaciones	16
5.24. Diapositiva 24. Permisos de aplicaciones - VIDEO.....	16
5.25. Diapositiva 25. Actividad 4	16
5.26. Diapositiva 26. Herramientas antirrobo	16
5.27. Diapositiva 27. Herramientas antirrobo Android.....	17
5.28. Diapositiva 28. Herramientas antirrobo iOS	17
5.29. Diapositiva 29. Gestión de la memoria del dispositivo	17
5.30. Diapositiva 30. Gestión de la memoria del dispositivo Android.....	17
5.31. Diapositiva 31. Gestión de la memoria del dispositivo iOS	18
5.32. Diapositiva 32. Actividad 5	18
5.33. Diapositiva 33. Guardando mis archivos en la nube de forma automática.....	18
5.34. Diapositiva 34. Guardando mis archivos en la nube de forma automática Android.....	18
5.35. Diapositiva 35. Guardando mis archivos en la nube de forma automática iOS	19
5.36. Diapositiva 36. <i>Rooting / Jailbreacking</i> del dispositivo	19
5.37. Diapositiva 37. <i>Rooting / Jailbreacking</i> del dispositivo	20
5.38. Diapositiva 38. En INCIBE te ayudamos.....	20
5.39. Diapositiva 39. Cuestionario de evaluación 1	20
5.40. Diapositiva 40. Cuestionario de evaluación 2	20
5.41. Diapositiva 41. Cuestionario de evaluación 3	20

5.42. Diapositiva 42. Cuestionario de evaluación 4	21
5.43. Diapositiva 43. Cuestionario de evaluación 5	21
5.44. Diapositiva 44. Cuestionario de evaluación 6	21
5.45. Diapositiva 45. Cuestionario de evaluación 7	21
5.46. Diapositiva 46. Cuestionario de evaluación 8	21
5.47. Diapositiva 47. Cuestionario de evaluación 9	21
5.48. Diapositiva 48. Cuestionario de evaluación 10.....	22
5.49. Diapositiva 49. Final del taller	22
6. Recursos de evaluación	23
6.1. Cuestionario de evaluación	24
ANEXO	27
Recursos para ampliar	27

1. OBJETO DEL DOCUMENTO

El presente documento constituye una herramienta didáctica que servirá de apoyo al docente para la planificación del **taller formativo de “Seguridad en dispositivos para sistemas operativos Android e iOS”**.

Esta herramienta supone un **instrumento específico de planificación, desarrollo y evaluación** de cada una de las áreas de las que se compone la acción formativa, y requiere de la labor docente para concretar los distintos elementos curriculares adaptándolos a las características del alumnado.

A lo largo de la guía docente, se profundizará en los **objetivos generales y específicos de la acción formativa, sus contenidos, criterios de evaluación y aquellos materiales y recursos adicionales** que se requieran para la impartición de las competencias recogidas en el taller.

2. ORGANIZACIÓN Y ESTRUCTURA

La estructura del taller estará compuesta por 11 temas que comprenderán los contenidos teóricos y actividades para el trabajo individual de cada alumno.

La estructura completa del taller es la siguiente:

1. **Bloqueo de pantalla.**
2. **Actualizaciones automáticas.**
3. **Software de seguridad.**
4. **Copias de seguridad.**
5. **Redes inalámbricas del dispositivo.**
6. **Descarga de aplicaciones desde un sitio seguro.**
7. **Permisos de aplicaciones.**
8. **Herramientas antirrobo.**
9. **Gestión de la memoria del dispositivo.**
10. **Guardando mis archivos en la nube de forma automática.**
11. **Rooting / Jailbreacking del dispositivo.**

3. OBJETIVO

Este taller tiene como objetivo principal el de: **proporcionar a los alumnos las competencias necesarias para gestionar la seguridad y protección de sus dispositivos a través de las opciones de configuración de sus sistemas (Android e iOS)**. Dado el enfoque teórico-práctico, así como el nivel de profundidad de sus contenidos, el taller va dirigido a un colectivo de usuarios con conocimientos muy básicos sobre tecnología y seguridad.

A lo largo del taller, se ofrecerá a los alumnos recursos de ampliación en forma de enlaces de la OSI, con el fin de expandir sus competencias y satisfacer su curiosidad. Del mismo modo, servirán al docente para enriquecer los contenidos del taller.

4. METODOLOGÍA Y RECURSOS

La metodología empleada en el desarrollo de este taller es de **carácter teórico-práctico, visual y buscando la participación activa del alumnado** durante la impartición del taller:

- **Teórico-práctica:** Los contenidos teóricos vendrán acompañados en todo momento de ejemplos reales que aterricen la teoría. A través de casos reales y actividades, el alumnado pondrá en práctica la información transmitida a través del taller.
- **Visual:** Las imágenes técnicas y decorativas abundarán a lo largo de todo el taller. Además, para dinamizar aún más los talleres, se incluirán recursos audiovisuales relacionados con el contenido (al menos 1 vídeo por taller).
- **Participación activa:** El alumnado tendrá un papel fundamental en los talleres, pues no se limitarán a escuchar. Los contenidos están preparados para que se pongan en práctica desde el comienzo del taller en cada uno de los equipos del alumnado.
 - Además, se busca enriquecer la experiencia formativa a través de las dudas y comentarios que se expongan durante su desarrollo.

El taller cuenta con diferentes **actividades y recursos** al servicio del docente para la impartición:

- **Presentación en Power-Point.** Se trata de una presentación con comentarios en texto para apoyar al docente, y los contenidos a compartir con el alumnado.
- **Actividades.** Se trata de pequeñas actividades que permiten al alumnado poner en práctica los conocimientos recién adquiridos, y que acompañan a los apartados principales.
- **Vídeos y enlaces para ampliar.** Servirán para afianzar los contenidos desarrollados mediante ejemplos y contenidos para ampliar con los que enriquecer la acción formativa.
- **Cuestionario de evaluación.** Cuestionario final del taller formado por 15 ítems con opción múltiple con el que realizar la evaluación final de los alumnos.

5. CONTENIDOS

A continuación, se muestra el contenido del taller ordenado en diapositivas para facilitar la tarea al docente.

5.1. Diapositiva 1. Presentación del taller

Presentación del taller “Seguridad en dispositivos: Android e iOS”. Debe mencionarse la labor de INCIBE y el teléfono de ayuda 017.

5.2. Diapositiva 2. Índice

Presentación del índice de contenidos del taller:

1. Bloqueo de pantalla.
2. Actualizaciones automáticas.
3. Software de seguridad.
4. Copias de seguridad.
5. Redes inalámbricas del dispositivo.
6. Descarga de aplicaciones desde un sitio seguro.
7. Permisos de aplicaciones.
8. Herramientas antirrobo.
9. Gestión de la memoria del dispositivo.
10. Guardando mis archivos en la nube de forma automática.
11. *Rooting / Jailbreacking* del dispositivo.
12. Cuestionario de evaluación.

5.3. Diapositiva 3. Introducción

Nuestros dispositivos son una parte fundamental hoy en día.

Su uso abarca desde navegar por Internet a realizar compras online, por ello es tan importante que **conozcamos algunas de sus funciones de seguridad básicas, así como las tareas de mantenimiento o configuraciones de seguridad que podemos llevar a cabo junto a los procesos automáticos que las mejoran.**

5.4. Diapositiva 4. Bloqueo de pantalla

Bloquear la pantalla de nuestro dispositivo parece algo evidente, pero es un hábito que no siempre cumplimos. De no hacerlo, **corremos el riesgo de que, en caso de pérdida o robo, una tercera persona tenga acceso a la información más desprotegida** almacenada en un dispositivo. De igual modo, si lo dejamos desbloqueado cerca de personas cercanas, nuestra privacidad quedaría expuesta.

A la hora de bloquear nuestro dispositivo y restringir el acceso al mismo por parte de terceros, lo mejor es **configurar un bloqueo de pantalla**. Existen diferentes tipos de bloqueo:

- **PIN:** se trata de un código numérico de entre cuatro y seis dígitos, dependiendo del sistema.
- **Contraseña:** es una clave alfanumérica con caracteres especiales.
- **Patrón:** permite utilizar un patrón de puntos formando una figura.

- **Biometría:** algunos dispositivos más modernos permiten bloquear y desbloquear el mismo a través de nuestra huella digital o, incluso, nuestro rostro.

5.5. Diapositiva 5. Bloqueo de pantalla

Para configurarlo en Android:

- Ir a **Ajustes > Seguridad > Bloqueo de pantalla**. Aquí podremos configurar el tipo de bloqueo de pantalla que queramos.

En el caso de un sistema **iOS**, podemos acceder a distintas funciones para configurar el bloqueo de pantalla:

- **Bloquear con código de seguridad:** accederemos a **Ajustes > Touch ID y código**. Si no tenemos ningún código configurado, haremos clic en **Activar código de acceso**. Podemos también modificarlo en **Cambiar código**.
- **Bloquear con Touch ID:** en el mismo menú, podemos seleccionar la función **Touch ID > Agregar una huella digital**.
- **Bloquear con Face ID:** en **Ajustes** encontraremos la opción **Face ID y código** (aunque depende de la versión del dispositivo). Una vez hayamos ingresado el código de seguridad, podremos configurar esta opción.
- **Bloqueo automático:** es recomendable que configuremos un tiempo límite para el bloqueo automático. Accederemos a **Ajustes > Pantalla y brillo > Bloqueo automático** para configurarlo.

5.6. Diapositiva 6. Actividad 1

Diapositiva para introducir a los usuarios la actividad. El tiempo aproximado de duración será de entre 3-5 minutos. Los pasos habrán sido descritos en las diapositivas anteriores.

La labor del docente será la de acompañar a los usuarios y ayudar en caso necesario. Se debe valorar la iniciativa, la resolución de la actividad y la proactividad.

Actividad 1:

Configurar el bloqueo de pantalla es una de las primeras opciones que debemos realizar cuando nos hacemos con un dispositivo nuevo. Sin embargo, es probable que podamos mejorar la configuración para hacerla más segura. ¿Por qué no lo intentamos?

5.7. Diapositiva 7. Actualizaciones automáticas

Las actualizaciones son fundamentales, ya que nos protegen de vulnerabilidades y errores o brechas en la seguridad de las aplicaciones y del sistema de nuestro dispositivo. Sin ellas, los atacantes podrían ingresar al sistema, infectarnos y robar información fácilmente.

Para asegurarnos de mantener nuestros dispositivos actualizados, lo más sencillo es configurarlos para realizar actualizaciones automáticas. Lo primero y más importante es asegurarnos de que nuestro dispositivo está conectado a Internet, preferiblemente a una red wifi.

- En **Android**, bastará con acceder a **Ajustes > Sistema > Ajustes avanzados > Actualización del sistema**. Si estamos desactualizados, solo deberemos seguir los pasos indicados. En otros modelos, será **Ajustes > Sobre el teléfono > Actualización del sistema**.
- En un sistema **iOS** iremos a **Ajustes > General y Actualización de software**. Es posible que nos pida el código de acceso de nuestra cuenta.

5.8. Diapositiva 8. Actualizaciones automáticas

También debemos mantener todas nuestras aplicaciones actualizadas:

- En el caso de **Android**, bastará con ingresar en Google Play y descargarnos las últimas versiones, aunque también podemos llevar a cabo actualizaciones automáticas desde **Ajustes > Actualizar aplicaciones automáticamente** (o un nombre similar) y configurarlo.
- Para actualizar las aplicaciones en **iOS**, abriremos la **App Store > Hoy** y pulsaremos el icono de nuestro perfil. Aquí podremos ver las actualizaciones pendientes que podremos instalar haciendo clic en **Actualizar** o **Actualizar todo**. Las actualizaciones automáticas pueden configurarse desde **Ajustes > ID Apple > iTunes Store y App Store** y activar la opción de **Actualizaciones de apps**.

5.9. Diapositiva 9. Actividad 2

Diapositiva para introducir a los usuarios la actividad. El tiempo aproximado de duración será de entre 3-5 minutos. Los pasos habrán sido descritos en las diapositivas anteriores.

La labor del docente será la de acompañar a los usuarios y ayudar en caso necesario. Se debe valorar la iniciativa, la resolución de la actividad y la proactividad.

Actividad 2:

Un dispositivo actualizado está mejor preparado para defender nuestros datos de los ciberataques. Aunque pensemos que funciona perfectamente, nunca está de más asegurarnos de disponer de la última versión disponible, comprobándolo desde la configuración del dispositivo.

5.10. Diapositiva 10. Software de seguridad

Existen miles de aplicaciones para los dispositivos móviles y, algunas de ellas, nos sirven para **mejorar la seguridad del dispositivo y nuestra privacidad**:

1. **Aplicaciones de antivirus**: su objetivo es detectar y eliminar los virus y *malware* que podemos haber descargado sin ser conscientes. También sirven para detectar posibles amenazas cuando navegamos por Internet o instalamos una app.
2. **Aplicaciones de cifrado**: con ellas podemos cifrar desde un archivo, carpeta, hasta todo el dispositivo. De este modo, solo nosotros que conocemos la contraseña, podremos acceder a toda la información cifrada.
3. **Bloqueo de aplicaciones**: este tipo de aplicaciones sirven para mejorar la protección de nuestra información más personal, evitando el acceso no autorizado de terceras personas a las apps en las que manejamos estos datos sensibles. Un ejemplo, son las aplicaciones de mensajería instantánea o las redes sociales.

5.11. Diapositiva 11. Software de seguridad

4. **Gestores de contraseñas:** su función es la de almacenar y ayudarnos a gestionar las contraseñas de una forma más segura, encriptándolas y sincronizándolas con otros dispositivos. Solo necesitaremos una clave maestra para tener a buen recaudo el resto de nuestras contraseñas. Algunas añaden funciones extra, como ayuda para crear contraseñas más robustas y avisándonos cuando no hemos cambiado una clave en mucho tiempo.
5. **Aplicaciones de verificación en dos pasos, o factor múltiple de autenticación:** nos ayudan a proteger nuestras cuentas, solicitando un tercer componente que, sumado al usuario y una contraseña robusta, añaden una capa extra de protección. Este tercer componente (o más) puede ser un código o clave generada aparte o un elemento biométrico, como nuestra huella.
6. **Aplicaciones de privacidad y navegación por Internet:** utilizar navegadores que incorporen mayores opciones de privacidad y seguridad, cómo un límite a los rastreadores, motores de búsqueda con declaraciones de privacidad más restrictivas o un modo incógnito por defecto, son una solución si lo que buscamos es mejorar la seguridad cuando navegamos por Internet.

5.12. Diapositiva 12. Software de seguridad

7. **Conan mobile, análisis del estado de seguridad del dispositivo:** además, desde INCIBE ofrecemos nuestra propia app para proteger dispositivos con sistema Android: [Conan mobile](#).

Nos permitirá conocer el estado de seguridad de nuestros dispositivos, mostrando posibles riesgos en su configuración y cómo solucionarlos. Además, verifica que no tengamos instalada ninguna app maliciosa, nos alerta en caso de detectar ciertas situaciones de riesgo, y nos proporciona consejos para mejorar nuestra seguridad.

Tanto Android, como iOS disponen, en sus tiendas oficiales, de aplicaciones con las funcionalidades anteriormente descritas. Algunas son comunes para ambos sistemas, aunque otras tendrán una versión para cada uno. Recuerda que la OSI pone a vuestra disposición una sección de [herramientas](#) donde podréis encontrar varias opciones para proteger vuestros dispositivos.

5.13. Diapositiva 13. Software de seguridad

8. **[El servicio AntiBotnet](#)** pone a disposición de los usuarios mecanismos para poder identificar si desde tu conexión a Internet (siempre que lo utilices dentro de España) se ha detectado algún incidente de seguridad relacionado con [botnets](#) u otras amenazas, ofreciéndote información y enlaces a herramientas que te pueden ayudar en la desinfección de tus dispositivos.

El Servicio Antibotnet se ofrece a los usuarios a través de cinco servicios diferentes:

- **Servicio Online:** Los usuarios pueden chequear online si su IP pública está infectada por un malware relacionado con una botnet.
- **Servicio Plugin:** Plugin disponible para Google Chrome, Firefox y Internet Explorer que chequea la IP de forma periódica y automática, con el fin de notificar al usuario en caso de que se detecte un resultado positivo.
- **CONAN Mobile:** Aplicación desarrollada por INCIBE para dispositivos Android, que ayuda a comprobar el nivel de seguridad de los dispositivos

móviles. Esta app integra la funcionalidad del Servicio Antibotnet, alertando en caso de que se detecte un resultado positivo en las redes wifi.

- **Notificación ISP:** El ISP Español, Telefónica, colabora notificando a los usuarios por email sobre incidentes relacionados con botnets que afecten a sus conexiones de internet. INCIBE facilita a Telefónica diariamente un feed que contiene las evidencias relativas a sus ASNs. Con esta información, Telefónica puede identificar los usuarios de las líneas afectadas y por tanto enviarles la notificación.
- **API para empresas:** API que permite al personal IT integrar el servicio en sus sistemas de monitorización de redes. Este servicio está orientado a empresas.

5.14. Diapositiva 14. Copias de seguridad

Las copias de seguridad permiten **mantener un doble de toda la información que tengamos almacenada en nuestro dispositivo**. Son una práctica muy útil, especialmente si se llevan a cabo de forma periódica, ya que permiten recuperar información más o menos actualizada ante un incidente de pérdida o robo de esta.

En los dispositivos móviles, los datos más sensibles de ser respaldados son los contactos, la agenda del correo y archivos personales, como fotos o vídeos.

5.15. Diapositiva 15. Copias de seguridad

Para hacerlo en **Android**, deberemos:

- Acceder a **Ajustes > Google > Hacer copia de seguridad**. Seleccionaremos **Crear una copia de seguridad** ahora y crearemos una copia de nuestros datos en **Google Drive**.

Para hacerlo en **iOS**:

- Iremos a **Ajustes > ID Apple > iCloud > Copia en iCloud**. Desde aquí podremos activar la **Copia en iCloud** para que se realicen automáticamente.
- Para hacer una copia manual bastará con seleccionar **Realizar copia de seguridad ahora**.

5.16. Diapositiva 16. Actividad 3

Diapositiva para introducir a los usuarios la actividad. El tiempo aproximado de duración será de entre 3-5 minutos. Los pasos habrán sido descritos en las diapositivas anteriores.

La labor del docente será la de acompañar a los usuarios y ayudar en caso necesario. Se debe valorar la iniciativa, la resolución de la actividad y la proactividad.

Actividad 2:

Configurar una copia de seguridad solo te llevará unos minutos y te dará la tranquilidad de disponer de una copia de tu dispositivo tal y como se encuentra en este momento. ¿A qué esperas?

5.17. Diapositiva 17. Redes inalámbricas del dispositivo

Nuestros dispositivos inalámbricos tienen la posibilidad de conectarse a una gran variedad de redes inalámbricas. Algunas sirven para tener conexión a Internet, realizar pagos con el mismo dispositivo o conectarse a otros para intercambiar archivos.

5.18. Diapositiva 18. Redes inalámbricas del dispositivo: Bluetooth

Bluetooth: viene incorporado en todos los dispositivos móviles y permite conectarnos con otro dispositivo para compartir archivos o emparejar determinados dispositivos, como auriculares inalámbricos.

- Tanto en **Android**, como en **iOS**, bastará con ir a **Ajustes > Bluetooth** para activar o desactivar esta función y acceder a su configuración.
Si bien es una función muy útil, su mayor riesgo está a la hora de que un dispositivo que no conocemos acabe sincronizándose al nuestro. Para evitarlo, una vez hayamos terminado, desactiva el Bluetooth.
- Recomendaciones:
 - Tener el dispositivo actualizado.
 - Encender el bluetooth sólo cuando se vaya a hacer uso.
 - Tener activado el modo oculto.
 - Borrar los dispositivos a los que se haya conectado previamente.
 - Rechazar el emparejamiento con dispositivos desconocidos.

5.19. Diapositiva 19. Redes inalámbricas del dispositivo: wifi

Wifi: permite navegar por Internet al conectarnos a una red wifi cercana a nuestro dispositivo.

- En Android e iOS, iremos a **Ajustes > Wi-Fi** para activar o desactivar esta función. Además, veremos todas las redes disponibles a nuestro alcance.

Una red abierta puede ser peligrosa e infectar nuestros dispositivos con todo tipo de *malware*. Además, corremos el riesgo de que un ciberdelincuente monitorice toda nuestra actividad online para hacerse con nuestros datos y credenciales.

El mejor consejo es no conectarnos a redes públicas a no ser que sea imprescindible, y siempre con una VPN. Además, no accederemos a nuestras cuentas o servicios más personales, como la cuenta bancaria, correo electrónico o redes sociales, para evitar que acaben en manos de terceros.

- Recomendaciones:
 - Mantener el dispositivo y aplicaciones actualizados.
 - Activar el firewall y el antivirus.
 - Desactivar la conexión automática a redes inalámbricas.
 - Desactivar la sincronización.
 - No intercambiar información sensible o realizar compras.
 - Conectarse a páginas con cifrado de seguridad <https://>
 - Comprobar que la red disponible es la oficial del lugar.
 - Utilizar una VPN.

5.20. Diapositiva 20. Redes inalámbricas del dispositivo: VPN

VPN: las Redes Privadas Virtuales o VPN son un servicio que protege nuestra privacidad al cifrar la conexión entre nuestro dispositivo y el servidor VPN, por lo que, si alguien interceptase esta comunicación, sería incapaz de leer la información.

Existen una gran variedad de servicios y aplicaciones en el mercado, gratuitas y de pago, y nos servirán como una capa extra de seguridad al conectarnos a redes wifi poco fiables.

5.21. Diapositiva 21. Redes inalámbricas del dispositivo: NFC

NFC: se trata de una tecnología inalámbrica de corto alcance que permite conectar dos dispositivos entre sí para intercambiar información, y realizar pagos.

- Desde **Android**, podemos activar o desactivar esta función desde **Ajustes > Conexiones > NFC**. Para realizar pagos, necesitaremos instalar la aplicación [Google Pay](#).
- En el caso de **iOS** esta función no puede activarse o desactivarse, aunque puede cambiar en próximos dispositivos, y sí permite añadir tarjetas a la *wallet* para realizar pagos con el NFC.

Desde INCIBE queremos recordar que, como medida de seguridad, una vez hayamos terminado de utilizar alguno de estos servicios, lo mejor es desactivarlos para evitar abrir una puerta de acceso a los ciberdelincuentes.

- Recomendaciones:
 - Establecer bloqueo de teléfono.
 - Establecer doble factor de autenticación.
 - Utilizar servicios “Encuentra mi dispositivo” o “Busca mi Iphone”. Localización, desactivación y borrado.
 - Activar NFC sólo cuando se vaya a hacer uso, si es posible.

5.22. Diapositiva 22. Descarga de aplicaciones desde un sitio seguro

Las aplicaciones son *software* que podemos instalar en nuestro dispositivo y que tienen muchísimas funcionalidades. Nos pueden ayudar a proteger mejor nuestros equipos o comunicarnos con nuestros amigos, pero antes de descargarnos cualquiera de ellas:

- **Descarga solo de tiendas oficiales.** Las plataformas [Google Play](#) y [App store](#) cuentan con medidas de seguridad para evitar aplicaciones fraudulentas, aunque nunca está de más andarse con ojo.
- **Revisa quién es el desarrollador de la app.** Las empresas o desarrolladores conocidos ofrecen más garantías de seguridad. Revisa su sitio web y sus otros trabajos para asegurarte de que se trata de uno seguro y profesional.
- **Echa un vistazo a los comentarios y valoraciones.** Si tiene pocos comentarios, y sus valoraciones son todas positivas o, por el contrario, si tiene muchos, pero son negativos. ¡Desconfía!
- **Comprueba el número de descargas.** Una app con un nombre famoso, pero que tiene pocas descargas debe hacernos sospechar que se podría tratar de una aplicación fraudulenta que se aprovecha del tirón de otra más conocida.

Una aplicación fraudulenta podría infectar nuestro dispositivo y tomar control de este. De modo que, tanto si utilizamos iOS o Android, recordaremos que, comprobar que se trata de una app fiable solo nos llevará unos minutos de más.

5.23. Diapositiva 23. Permisos de aplicaciones

Cuando vamos a instalar una aplicación, esta nos pedirá una serie de permisos para funcionar. Lo más recomendable es leerlos detenidamente y, si no estamos seguros o no parecen necesarios para el funcionamiento de la app, no darlos. Una app maliciosa tratará de pedir todos los permisos posibles para poder actuar con libertad en nuestro dispositivo.

Para gestionar los permisos en **Android**, haremos lo siguiente:

- Iremos a **Ajustes > Aplicaciones > Permisos**.
- Dentro, podremos ver una lista con todos los permisos que hemos concedido a las aplicaciones. Haciendo clic sobre ellos, **podremos** ver a qué aplicación concreta se lo hemos concedido y gestionarlos.

Desde un sistema **iOS**, deberemos:

- Ir a **Ajustes**. Al final, veremos las apps instaladas. Si hacemos clic en ellas podremos ver los permisos que se han concedido a la aplicación.

5.24. Diapositiva 24. Permisos de aplicaciones - VIDEO

En esta diapositiva se compartirá con los usuarios un vídeo que representará los pasos anteriormente descritos para revisar los permisos dados a las aplicaciones instaladas en sus dispositivos Android e iOS. La duración será de 1 min. aproximadamente.

5.25. Diapositiva 25. Actividad 4

Diapositiva para introducir a los usuarios la actividad. El tiempo aproximado de duración será de entre 3-5 minutos. Los pasos habrán sido descritos en las diapositivas anteriores.

La labor del docente será la de acompañar a los usuarios y ayudar en caso necesario. Se debe valorar la iniciativa, la resolución de la actividad y la proactividad.

Actividad 4:

Seguro que tienes alguna aplicación instalada. Te invitamos a que accedas a tu dispositivo móvil y analices los permisos que diste a la última aplicación instalada. Prueba a revocar alguno si no lo ves necesario.

5.26. Diapositiva 26. Herramientas antirrobo

Con la funcionalidad GPS activada muchas aplicaciones pueden recopilar y compartir nuestra ubicación y, aunque en ocasiones pueda suponer un riesgo para nuestra privacidad, si la utilizamos con cabeza, también puede ayudarnos a encontrar un dispositivo extraviado, o localizar a una persona en paradero desconocido.

Aquí entran las herramientas antirrobo que actúan rápidamente en caso de pérdida o robo de nuestro dispositivo.

5.27. Diapositiva 27. Herramientas antirrobo Android

En el caso de **Android**, disponemos de la opción **Administrador de dispositivos**. Esta herramienta nos permitirá encontrar el teléfono geográficamente.

- Iremos a **Ajustes > Estado de seguridad / Seguridad y ubicación o Google > Seguridad**. Nos aseguraremos de que la función [Encontrar dispositivo](#) esté activada y actualizada.
- Para ello, iremos a **Ajustes > Ubicación** y a activar. Luego, deberemos darle visibilidad a nuestro dispositivo en [Google Play](#). De este modo, si perdemos o nos roban el teléfono, podremos localizarlo fácilmente.
- Podemos comprobar que la herramienta funciona desde: <https://android.com/find>.

5.28. Diapositiva 28. Herramientas antirrobo iOS

Con **iOS** podemos utilizar la función **Buscar mi iPhone/iPad** para compartir la ubicación de tu dispositivo con otras personas. Para configurar esta funcionalidad:

- Iremos a **Ajustes > Privacidad > Localización** para activarla.
- Si queremos localizarlo, aunque esté desactivado, activaremos **Permitir localización sin conexión**. Y, si queda poca batería, activaremos **Enviar última ubicación**.
- Después, volveremos a **Ajustes > [nombre] > Buscar** para activar la opción **Buscar mi iPhone/iPad**.
- Podemos probar esta función ingresando con nuestra cuenta de Apple en: <https://www.icloud.com/find>

5.29. Diapositiva 29. Gestión de la memoria del dispositivo

Nuestro dispositivo tiene una memoria limitada que se va llenando a medida que instalamos aplicaciones y guardamos información en él. Si el dispositivo lo permite, se puede ampliar su capacidad total mediante tarjetas de memoria microSD.

- **Memoria interna:** es aquella que se incluye en el teléfono.
- **Memoria externa:** es la que podemos ampliar a base de tarjetas microSD.

5.30. Diapositiva 30. Gestión de la memoria del dispositivo Android

Para disponer de una visión más detallada y gestionar la memoria de nuestro **dispositivo Android**, iremos a **Ajustes > Sobre el teléfono > Almacenamiento**.

Si queremos liberar espacio de las aplicaciones y sus datos:

- Desde **Ajustes > Aplicaciones > Administrar aplicaciones** podremos eliminar las que ya no queramos. También podemos borrar sus datos para liberar algo de espacio sin llegar a borrarla del todo.
 - **Borrar caché:** elimina los datos temporales. Algunas apps pueden tardar más en abrirse la próxima vez que las utilices.
 - **Borrar datos:** elimina de forma permanente todos los datos de la app.

Si queremos liberar espacio de archivos como imágenes, vídeos o audio:

- Iremos a **Archivos o Gestor de archivos**.

- Dentro, seleccionaremos los distintos tipos de archivos que queramos eliminar y haremos clic en **Eliminar**.

De vez en cuando conviene revisar las aplicaciones y archivos almacenados para asegurarnos de eliminar aquellos que no queremos o no necesitamos.

5.31. Diapositiva 31. Gestión de la memoria del dispositivo iOS

En el caso de iOS, podemos consultar el almacenamiento desde **Ajustes > General > Almacenamiento del dispositivo**. Dentro, dispondremos de algunas recomendaciones para liberar espacio, como **Desinstalar apps no utilizadas**. También veremos las apps instaladas y su peso, para que elijamos las que queremos desinstalar:

- **Desinstalar app**: liberará espacio de almacenamiento, pero se conservarán algunos datos de la aplicación.
- **Eliminar app**: se eliminará completamente la aplicación del dispositivo.

5.32. Diapositiva 32. Actividad 5

Diapositiva para introducir a los usuarios la actividad. El tiempo aproximado de duración será de entre 3-5 minutos. Los pasos habrán sido descritos en las diapositivas anteriores.

La labor del docente será la de acompañar a los usuarios y ayudar en caso necesario. Se debe valorar la iniciativa, la resolución de la actividad y la proactividad.

Actividad 5:

Si descuidamos la memoria de nuestro dispositivo, puede que acabemos quedándonos sin espacio muy pronto. Ya sean fotografías vídeos o apps que no utilizas, una limpieza a tiempo te ayudará en el futuro. Accede a la configuración y haz una limpieza ligera para disponer de espacio suficiente para futuras actualizaciones de seguridad, por ejemplo.

5.33. Diapositiva 33. Guardando mis archivos en la nube de forma automática

La nube nos permite disponer de un servicio de almacenamiento en la Red para no tener que estar constantemente eliminando u organizando la información de nuestro dispositivo.

Además, nos permite disponer de un lugar donde **almacenar nuestras copias de seguridad**. Para mayor comodidad, podemos sincronizar nuestros archivos y subirlos de forma automática a la nube.

5.34. Diapositiva 34. Guardando mis archivos en la nube de forma automática Android

Android: gracias a nuestra cuenta de Google tendremos acceso al almacenamiento en la nube de Google Drive y Google Fotos. Este espacio de almacenamiento extra nos servirá para guardar nuestras copias de seguridad, fotografías y vídeos, etc.

Por defecto, Google subirá a la nube una copia de seguridad de muchos de los datos que tengamos asociados a nuestro dispositivo móvil mediante la sincronización. Si queremos saber lo que se está subiendo continuamente, iremos a **Ajustes, Cuenta y sincronización/Cuentas > Google**. Desde ahí, podremos configurarlo a nuestro gusto.

En el caso de que queramos utilizar el almacenamiento para guardar nuestros archivos personales, es tan sencillo como:

- Ir a **Archivos/Gestor de archivos**, seleccionar los que queramos guardar y hacer clic en **Enviar**.
- Luego, seleccionamos **Google Drive** o **Google Fotos** y listo.

De esta forma, podremos liberar espacio en nuestro dispositivo, disponer de una copia de seguridad y proteger nuestros archivos e información más preciada.

5.35. Diapositiva 35. Guardando mis archivos en la nube de forma automática iOS

iOS: Apple también dispone de su propio servicio en la nube conocido como iCloud. Desde nuestros dispositivos podemos sincronizarlos para subir todos nuestros archivos automáticamente- Para ello:

- Iremos a **Configuración > ID Apple > iCloud Drive** para activarlo.
- Para gestionar nuestros archivos de iCloud Drive necesitaremos la [app Archivos](#). Desde esta, podremos configurar la subida de archivos a la nube fácilmente.

5.36. Diapositiva 36. *Rooting / Jailbreacking* del dispositivo

Estos términos hacen referencia a procedimientos mediante los cuales pueden 'liberarse' los dispositivos móviles, como *smartphones* o *tablets*, eliminando las restricciones que los fabricantes llevan a cabo en los dispositivos:

- **Rooting (Android):** Mediante este proceso conseguimos acceso '*root*' al dispositivo, es decir, obtener permisos de 'superusuario' o administrador, con los que tendremos acceso al sistema sin ningún tipo de restricción. Una de sus ventajas es la de poder darle permisos de administrador a una aplicación, lo que permitirá que ésta desinstale otras apps o elimine permisos, por ejemplo.
- **Jailbreaking (iOS):** se trata del proceso con el que conseguimos eliminar las limitaciones impuestas por Apple en un dispositivo con iOS. Una vez 'liberado', podemos, por ejemplo, instalar aplicaciones de terceros que no estén en la App Store.

De este modo, **podremos acceder con un perfil de administrador y disponer de los máximos privilegios posibles**. Algunos de estos privilegios son:

- Acceder a datos/carpetas protegidos.
- Instalar nuevas versiones de Android, incluso las no testadas o experimentales.
- Modificación de otros parámetros, como el inicio del dispositivo.
- Acceder a nuevas funcionalidades del *hardware* o de los sensores del dispositivo.

5.37. Diapositiva 37. *Rooting / Jailbreacking* del dispositivo

Aunque esto tiene un coste, y es exponernos a una **gran variedad de riesgos** que pueden vulnerar nuestra seguridad:

- Puede dar **problemas con la garantía** al haberse realizado modificaciones en el *software* instalado de raíz.
- Puede hacer al **sistema menos estable**. Por ejemplo, al realizar modificaciones en la configuración base del dispositivo o instalar versiones de Android no testadas o en fase Beta.
- Puede exponerse más a **infecciones por malware**. Determinadas configuraciones podrían inutilizar o dejar mermadas algunas funciones de seguridad del dispositivo.

Existen otros muchos riesgos por lo que, desde INCIBE, no recomendamos llevar a cabo ninguno de estos procedimientos a no ser que seas un usuario avanzado con conocimientos técnicos, y que sepas muy bien lo que haces.

5.38. Diapositiva 38. En INCIBE te ayudamos

Mostramos la información de INCIBE prestando especial atención a la Línea de Ayuda en Ciberseguridad de INCIBE a través de la cual cualquier menor o adulto puede contactar de manera gratuita y confidencial cuando tengan una duda o un problema en Internet, llamando al número de teléfono 017 o enviando un mensaje a través de la página web <https://www.incibe.es/linea-de-ayuda-en-ciberseguridad>.

Animamos a los participantes a visitar las diferentes webs de INCIBE en función del público (Ciudadanos, Menores o Empresas) y a seguirnos en redes sociales.

Además, explicamos que en la web pueden encontrar mucha información y actividades para trabajar cualquier tema de ciberseguridad, juegos y recursos pedagógicos.

5.39. Diapositiva 39. Cuestionario de evaluación 1

Lo más recomendable a la hora de crear cuentas en un sistema es:

- A. Biometría.
- B. Patrón.
- C. TouchID.

5.40. Diapositiva 40. Cuestionario de evaluación 2

El patrón de desbloqueo de nuestra pantalla mediante el uso de nuestra huella dactilar se conoce como:

- A. Para solucionar posibles vulnerabilidades.
- B. Para disponer de la última versión de nuestros programas favoritos.
- C. Para mejorar el rendimiento de nuestro sistema.

5.41. Diapositiva 41. Cuestionario de evaluación 3

Las copias de seguridad nos permiten:

- A. Proteger la información en caso de pérdida, daño o robo.
- B. Optimizar los recursos del sistema.

C. Mejorar la seguridad de nuestras aplicaciones.

5.42. Diapositiva 42. Cuestionario de evaluación 4

¿Cómo se conoce a la tecnología inalámbrica que permite realizar pagos con nuestro dispositivo móvil?

- A. VPN.
- B. Google Pay.
- C. NFC.

5.43. Diapositiva 43. Cuestionario de evaluación 5

¿Cuál de las siguientes opciones no nos sirve para identificar posibles apps maliciosas?

- A. Revisar las valoraciones de otros usuarios.
- B. Revisar si dispone de micropagos.
- C. Comprobar el número de descargas.

5.44. Diapositiva 44. Cuestionario de evaluación 6

¿Cuál sería la postura correcta cuando una aplicación nos pide permisos antes de instalarse?

- A. No aceptar ninguno.
- B. Aceptarlos todos, si es de tienda oficial.
Aceptar solo los relacionados con su función.

5.45. Diapositiva 45. Cuestionario de evaluación 7

Si almacenamos fotos o vídeos en la memoria de la tarjeta microSD que tenemos insertada en nuestro dispositivo, hablamos de:

- A. Memoria externa.
- B. Memoria interna.
- C. Memoria de terceros.

5.46. Diapositiva 46. Cuestionario de evaluación 8

De las siguientes opciones, ¿cuál no es un buen uso de la nube?

- A. Como almacén de nuestros datos más personales.
- B. Como almacén de nuestras copias de seguridad.
- C. Como almacén para liberar espacio de nuestro dispositivo.

5.47. Diapositiva 47. Cuestionario de evaluación 9

¿Cómo se conoce al procedimiento mediante el cual podemos “liberar” nuestro dispositivo móvil?

- A. Rooting / Freemobile.
- B. Scrooting / Jailbreacking.

C. *Rooting / Jailbreacking.*

5.48. Diapositiva 48. Cuestionario de evaluación 10

¿Cuál de los siguientes no es un riesgo vinculado a liberar nuestro dispositivo móvil?

- A. Ausencia de herramientas de protección.
- B. Problemas con la garantía
- C. Mayor riesgo de infección por malware.

5.49. Diapositiva 49. Final del taller

¡Gracias por vuestra atención!

6. RECURSOS DE EVALUACIÓN

Las herramientas de evaluación del alumnado permitirán controlar la calidad del aprendizaje recibido, gracias a una serie de **criterios de evaluación**:

1. **Participación durante el taller.** La participación del alumnado mediante dudas u otro tipo de aportaciones, resulta de un gran valor evaluativo (10% de la evaluación final).
2. **Actividades.** Estas actividades situadas al final de la mayoría de los apartados son uno de los medios de mayor potencial para la asimilación de las competencias recogidas en el taller. Además, permitirá al docente recibir u feedback directo sobre la evolución del alumnado (25% de la evaluación final).

1	Configurar el bloqueo de pantalla es una de las primeras opciones que debemos realizar cuando nos hacemos con un dispositivo nuevo. Sin embargo, es probable que puedas mejorar la configuración para hacerla más segura. ¿Por qué no lo intentamos?
2	Un dispositivo actualizado está mejor preparado para defender nuestros datos de los ciberataques. Aunque pensemos que funciona perfectamente, nunca está de más asegurarnos de disponer de la última versión disponible comprobándolo desde la configuración del dispositivo.
3	Configurar una copia de seguridad solo te llevará unos minutos y te dará la tranquilidad de disponer de una copia de tu dispositivo tal y como se encuentra en este momento. ¿A qué esperas?
4	Seguro que tienes alguna aplicación instalada. Te invitamos a que accedas a tu dispositivo móvil y analices los permisos que diste a la última aplicación instalada. Prueba a revocar alguno si no lo ves necesario.
5	Si descuidamos la memoria de nuestro dispositivo, puede que acabemos quedándonos sin espacio muy pronto. Ya sean fotografías vídeos o apps que no utilizas, una limpieza a tiempo te ayudará en el futuro. Accede a la configuración y haz una limpieza ligera para disponer de espacio suficiente para futuras actualizaciones de seguridad, por ejemplo.

3. **Cuestionario de evaluación.** Este instrumento de evaluación proporcionará gran parte de la puntuación final del alumnado y pondrá a prueba a los alumnos al finalizar un taller (65% de la evaluación final).

EVALUACIÓN FINAL = Participación + Actividades aprendizaje + Cuestionario de evaluación

6.1. Cuestionario de evaluación

El cuestionario de evaluación está compuesto por 10 preguntas de tipo test “opción múltiple” (3 opciones). La respuesta correcta está destacada en color verde.

1	El patrón de desbloqueo de nuestra pantalla mediante el uso de nuestra huella dactilar se conoce como:	Biometría.
		Patrón.
		TouchID.
	Feedback: La respuesta correcta es Biometría. No todos los dispositivos lo permiten, pero su función es la de ejecutar determinadas funciones, como es bloquear o desbloquear la pantalla a partir de algún elemento que forme parte de nosotros, como la huella, el rostro o la voz.	
2	¿Para qué sirven las aplicaciones de cifrado?	Para cifrar todos nuestros archivos.
		Para detectar y eliminar posibles virus.
		Para mejorar el rendimiento del dispositivo.
	Feedback: La respuesta correcta es Para cifrar todos nuestros archivos. Así, podremos cifrar desde cualquier archivo, carpetas e incluso todo el dispositivo y protegerlos de terceros.	
3	Las copias de seguridad nos permiten:	Proteger la información en caso de pérdida, daño o robo.
		Optimizar los recursos del sistema.
		Mejorar la seguridad de nuestras aplicaciones.
	Feedback: La respuesta correcta es Proteger nuestra información en caso de pérdida, daño o robo. Ya que no solamente nos protegen de terceros, también de un borrado de archivos accidental.	
4	¿Cómo se conoce a la tecnología inalámbrica que permite realizar pagos con nuestro dispositivo móvil?	NFC.
		VPN
		Google Pay
	Feedback: La respuesta correcta es NFC. Esta tecnología de corto alcance permite que dos dispositivos se conecten entre sí para intercambiar información, e incluso para realizar pagos.	
5	¿Cuál de las siguientes opciones no nos sirve para identificar posibles apps maliciosas?	Revisar si dispone de micropagos.

		Revisar las valoraciones de otros usuarios.
		Comprobar el número de descargas.
	Feedback: La respuesta correcta es Revisar si dispone de micropagos. Esto no nos sirve para identificar una app maliciosa. Para ello, debemos revisar a la empresa desarrolladora, los comentarios y valoraciones de los usuarios y comprobar el número de descargas.	
6	¿Cuál sería la postura correcta cuando una aplicación nos pide permisos antes de instalarse?	Aceptar solo los relacionados con su función.
		No aceptar ninguno.
		Aceptarlos todos, si es de tienda oficial.
	Feedback: La respuesta correcta es Aceptar solo los relacionados con su función. De este modo, evitaremos que tengan control sobre determinadas funcionalidades. Por ejemplo, nunca le daríamos permisos para acceder a nuestros contactos a una app de linterna, ¿verdad?	
7	Si almacenamos fotos o vídeos en la memoria de la tarjeta microSD que tenemos insertada en nuestro dispositivo, hablamos de:	Memoria externa.
		Memoria interna.
		Memoria de terceros.
	Feedback: La respuesta correcta es Memoria externa. Es aquella que podemos ampliar a base de tarjetas como las microSD.	
8	De las siguientes opciones, ¿cuál no es un buen uso de la nube?	Como almacén de nuestros datos más personales.
		Como almacén de nuestras copias de seguridad.
		Como almacén para liberar espacio de nuestro dispositivo.
	Feedback: La respuesta correcta es Como almacén de nuestros datos más personales. Si bien es posible cifrarlos y mantenerlos a salvo de tercero, el uso más adecuado de la nube es para almacenar nuestras copias de seguridad y para liberar espacio de nuestro dispositivo con archivos que no queremos perder.	
9	¿Cómo se conoce al procedimiento mediante el cual podemos “liberar” nuestro dispositivo móvil?	Rooting / Jailbreacking.
		Rooting / Freemobile.
		Scrooting / Jailbreacking.
	Feedback: La respuesta correcta es Rooting o Jailbreacking. Estos procedimientos permitirán eliminar las restricciones de los fabricantes sobre nuestros dispositivos liberándolos, pero también dejándolos más expuestos.	

10	¿Cuál de los siguientes no es un riesgo vinculado a liberar nuestro dispositivo móvil?	Ausencia de herramientas de protección.
		Problemas con la garantía.
		Mayor riesgo de infección por malware.
	Feedback: La respuesta correcta es Menor rendimiento. Los principales riesgos de llevar a cabo estos procedimientos son los problemas con la garantía, un mayor riesgo de infección, la imposibilidad de actualizarlo de forma oficial y que puede hacer al sistema menos estable.	

ANEXO

RECURSOS PARA AMPLIAR

Se recomienda la lectura de la siguiente selección de recursos complementarios, por parte del docente:

- [La importancia de las actualizaciones de seguridad.](#)
- [Antivirus siempre activados y actualizados.](#)
- [¿Qué nos ofrece realmente un antivirus?](#)
- [Campaña ¡Contraseñas seguras!](#)
- [Campaña ¿Es seguro dónde guardas y cómo envías la información?](#)
- [Riesgos asociados al uso de redes inalámbricas no seguras.](#)
- [Redes wifi públicas: conéctate con prudencia.](#)
- [Fallos de seguridad en Bluetooth pueden ser utilizados para infectar dispositivos.](#)