Universitat d'Alacant
Universidad de Alicante

# PROTECCIÓN DE TUS DISPOSITIVOS

BUA

CID
COMPETENCIAS EN INFORMACIÓN DIGITAL

# ÍNDICE

# PROTECCIÓN DE TUS DISPOSITIVOS

## OBJETIVOS

- Conocer los riesgos asociados a los dispositivos móviles
- Aprender las medidas de protección a aplicar
- Ofrecer herramientas de seguridad que te ayudarán a proteger tus dispositivos

Consultar el correo, acceder a una hoja de cálculo o hacer una modificación a última hora de un documento importante, desde cualquier lugar, son solo algunas de las tareas que se pueden llevar a cabo desde los dispositivos móviles. En la actualidad, estos aparatos se han convertido en herramientas imprescindibles para el trabajo o el estudio, gracias a su movilidad y su conexión a Internet.

**Ordenadores portátiles, smartphones** o **tablets** te permiten desempeñar tu trabajo o estudio en cualquier sitio, como si estuvieras en las instalaciones de la universidad, lo que ha abierto un abanico nuevo de posibilidades, pero también nuevos riesgos que como usuario o usuaria debes tener en cuenta.


*Pexels-Drew Williams*

# RIESGOS ASOCIADOS

Los dispositivos móviles, tabletas y portátiles debido a su reducido tamaño y a la capacidad que tienen de gestionar tu información personal y académica, entrañan nuevos riesgos. Además de utilizar dispositivos móviles, te conectas desde el exterior de la red de la universidad, utilizas servicios para compartir documentos y contamos con riesgos asociados a entornos de trabajo no tan controlados.

*Flaticon- Riesgos*

## PRINCIPALES RIESGOS ASOCIADOS A LOS DISPOSITIVOS MÓVILES

- El **robo o pérdida** de los móviles, tabletas, portátiles y dispositivos de almacenamiento como discos duros externos y pendrives.
- La **infección por malware** o software malicioso, ya que puede robar información confidencial y credenciales de acceso a diferentes recursos.
- Los **sitios web fraudulentos**, la publicidad agresiva o las páginas web de tipo phishing son las principales amenazas a las que se exponen. Navegar en dispositivos pequeños, particularmente en móviles, entraña riesgos al ser más difícil «librarse» de esta publicidad.

- Utilizar **redes wifi inseguras** puede poner en riesgo la privacidad de las comunicaciones, ya que los ciberdelincuentes pueden estar «escuchando» todo lo que se envía y recibe.
- **Instalar aplicaciones** que necesitan acceder a determinados permisos del dispositivo, en ocasiones excesivos o innecesarios (como acceso a la cámara, los contactos o los archivos), para poder funcionar con normalidad.
- Dispositivos que **no cuentan con controles de acceso robustos** que los protejan. La ausencia de los mismos o el uso de algunos considerados débiles, como el patrón de bloqueo, son un riesgo para tu seguridad.
- La **falta de actualización,** tanto del **sistema operativo**, como de las aplicaciones supone un riesgo para la seguridad de toda la información que gestionan.
- La **modificación de los controles de seguridad impuestos por los fabricantes**. Si decides rootear o hacer jailbreak a alguno de tus dispositivos, puede suponer un grave riesgo, ya que los controles de seguridad impuestos por el desarrollador son eliminados.
- Establecer que el dispositivo o la aplicación **recuerde la contraseña**. Si un tercero accede al dispositivo tendría acceso a todos los servicios en los que estuviera guardada la contraseña.

## MEDIDAS DE PROTECCIÓN

Para contrarrestar los riesgos mencionados, es recomendable aplicar las siguientes medidas de protección:

### PROTECCIÓN ANTIMALWARE Y SITIOS WEB PELIGROSOS

Es importante disponer de herramientas que detecten y eliminen el software malicioso. Por otra parte, los **sistemas antivirus** siempre deberán estar **actualizados a la última versión**, algo que propiciará la identificación del malware más actual.

Es común que los antivirus también cuenten con herramientas que permitan identificar posibles sitios web fraudulentos o peligrosos, como aquellos utilizados para cometer phishing. Al seleccionar un antivirus para el móvil verifica que disponga de estas funcionalidades.

⚠ Es muy importante mantener el dispositivo actualizado, ya que te garantiza una seguridad más eficaz.

## PROTECCIÓN FRENTE ACCESOS NO DESEADOS

La primera barrera de seguridad para proteger la privacidad de tus dispositivos móviles está basada en **contraseñas y patrones de desbloqueo** del dispositivo.

⚠ Es fundamental que las claves de desbloqueo y acceso sean robustas (difíciles de romper), no predecibles y secretas.

En la **Guía de privacidad y la seguridad en internet**, realizada por la Agencia Española de Protección de Datos (AEPD), el Instituto Nacional de Ciberseguridad (INCIBE) y la Oficina de Seguridad del Internauta (OSI), se enumeran **consejos y recomendaciones sobre contraseñas, patrones y gestores de contraseñas.**

La función de *«Recordar contraseña»* **no** debe **usarse nunca en dispositivos móviles**, ya que ante un acceso no autorizado se podría acceder a todos los servicios donde se haya activado esta función.

Además, es recomendable configurar el terminal para que se **bloquee de forma automática** tras un tiempo de inactividad. De esta forma se mitigan las amenazas a las que se puede ver expuesta tu privacidad por posibles descuidos.

## PROTECCIÓN DE LA INFORMACIÓN

La información que se gestiona desde los dispositivos móviles o portátiles que se utilizan para el trabajo o estudio diario puede ser de gran importancia, por lo que protegerla será prioritario.

Para ello, se recomienda **activar el cifrado de la información en el dispositivo**. Todos los sistemas operativos deberán contar con herramientas de cifrado que protejan la información en ellos alojada. Los actuales sistemas operativos móviles como Android e iOS cuentan con cifrado de la información por defecto, pero los sistemas operativos para ordenador no, por lo que se debe activar.

## APLICACIONES LEGÍTIMAS

Las aplicaciones para dispositivos móviles deben ser **descargadas**, únicamente, desde la **tienda oficial**. Para teléfonos inteligentes y tabletas estas deben ser descargadas desde la App Store para Apple o desde Play Store para Android. En caso de ordenadores, como ya se indicó anteriormente, deben ser descargadas desde el sitio web oficial.

Todo el software utilizado y sistemas operativos deberán estar actualizados **a la última versión disponible.**

## NO UTILIZAR REDES WIFI INSEGURAS

Como estudiante de la UA, te recomendamos que **hagas uso de EDUROAM,** la **red inalámbrica de la Universidad de Alicante**. Para utilizarla debes activarla previamente en UACloud. Sigue los **pasos** que desde esta página web del Servicio de Informática te indican.

Es muy importante que tengas en cuenta:

- Conectando a la red inalámbrica, tu usuario/a debes escribirlo en minúsculas.
- Dispositivos móviles que no soportan eduroam.
- En caso de que necesites ayuda, puedes obtenerla en las "Preguntas Frecuentes".

Fuera de la UA, te vas a encontrar con distintos establecimientos y servicios públicos que ofrecen conexión wifi de manera gratuita a sus clientes. A pesar del ahorro que pueda suponerte, **no es recomendable utilizar estas conexiones wifi,** ya que no conoces su seguridad, ni su legitimidad (podrían fácilmente haberlas suplantado) y la privacidad de la información que envíes o recibas puede verse comprometida.

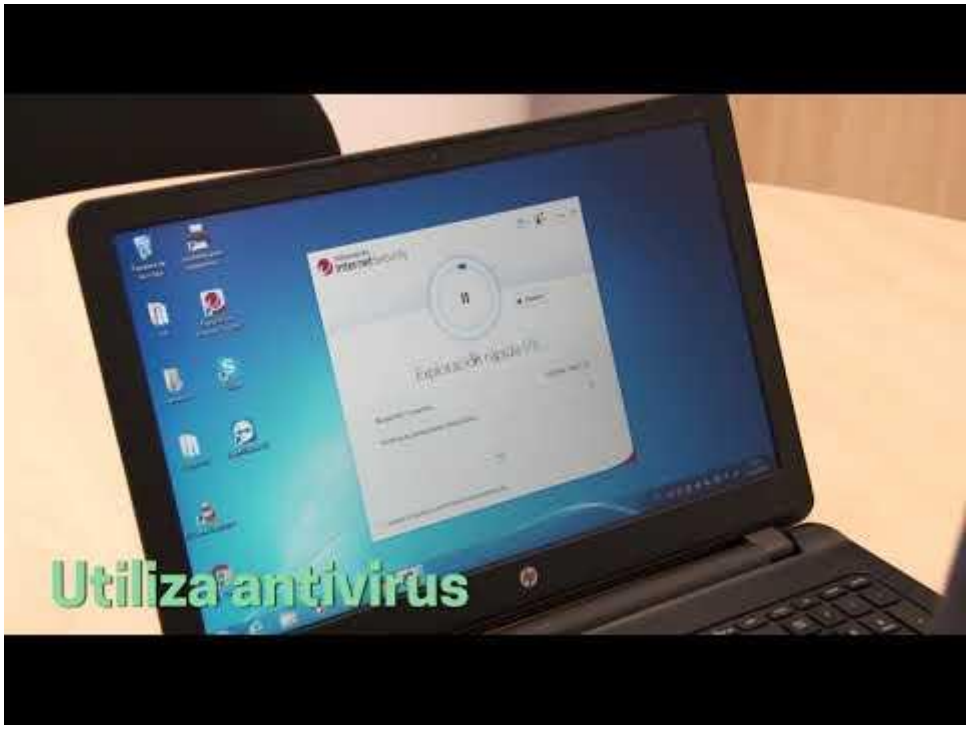
Siempre es mejor opción **utilizar la conectividad móvil 4 o 5 G** que incorporan los dispositivos (conexión de datos), especialmente cuando se realizan tareas sensibles como acceder a banca online o a información que pueda ser confidencial.

Y ten en cuenta, que cuando tus tareas académicas se tienen que trasladar al hogar, es fundamental seguir manteniendo un aceptable nivel de ciberseguridad:

- realizar copias de seguridad de forma periódica

- utilizar una conexión wifi-doméstica que puedas configurar de forma segura

PARA SABER MÁS




REBIUN Línea 2 (3er. P.E.) Grupo de Competencia Digital. *Protección de dispositivos* (CC BY-NC)

## HERRAMIENTAS DE PROTECCIÓN

En la **página web de la Oficina de Seguridad del Internauta,** ponen a tu disposición una serie de **herramientas de seguridad** que te ayudarán a proteger tus dispositivos, la información que almacenan, las comunicaciones utilizadas para el intercambio de información, además de otras muchas funcionalidades que pueden ser de tu interés.

Son las siguientes:

## ANTIVIRUS Y CLEANERS

- **Antivirus**: para detectar y eliminar virus y otras amenazas en tiempo real
- **Cleaner**: cuando sospechas que tu dispositivo ya está infectado

Antivirus y cleaners

## GESTORES DE CONTRASEÑAS

Para que puedas almacenar todas tus **contraseñas robustas y cifradas** de tal forma que sólo tengas que memorizar una, la que te da acceso al resto de contraseñas guardadas.

Gestores de contraseñas

## DOBLE FACTOR DE AUTENTICACIÓN

Si quieres dotar de **mayor seguridad a tus cuentas de usuario o usuaria,** para que tú y solo tú puedas acceder a ellas. Además de la contraseña, necesitarás un código que sólo tú recibirás a través del teléfono móvil.

Doble factor de autenticación

## CORTAFUEGOS (FIREWALL)

Para controlar las conexiones que se establecen entre tu dispositivo e Internet y vigilar quién puede acceder a la información guardada en tu equipo y qué es lo que sale de él, bloqueando toda aquella conexión que no autorices.

Cortafuegos (Firewall)

## ANALIZADORES DE URL Y ARCHIVOS

Cuando necesites comprobar si un archivo que recibes es malicioso o una página web es fraudulenta. Detectan rápidamente cualquier tipo de amenaza antes de que te afecte, así evitarás muchos problemas.

Analizadores de URL y archivos

## MANTENIMIENTO DE ARCHIVOS

Para que tus equipos funcionen bien es importante que dispongan de espacio libre en disco. Por eso es útil eliminar archivos duplicados, identificar aquellos grandes, etc. Estas aplicaciones ayudan a mantener el consumo del disco.

Mantenimiento de archivos

## CIFRADO

Seguro que almacenas información que no quieres que vea nadie excepto aquellas personas que tú autorizas. Para evitar que alguien acceda a ella sin tu permiso y pueda ver su contenido, cífrala con una contraseña.


## BORRADO SEGURO

Si vas a vender, prestar o tirar un dispositivo y quieres eliminar información de manera permanente, es decir, si no quieres que se pueda recuperar de ningún modo, haz uso de estas herramientas.

## RECUPERACIÓN DE ARCHIVOS

Si has borrado información que te gustaría recuperar por algún motivo, las herramientas de recuperación de datos pueden ayudarte en esta misión para que vuelvas a disfrutar de tus archivos perdidos y que recuperes su control.

Recuperación de archivos

## ANTIRROBO

Funcionalidades como la geolocalización del dispositivo o borrado de toda la información que contiene de forma remota pueden ser muy útiles en caso de pérdida o robo de tu dispositivo móvil. Configúrate una y adelántate a posibles riesgos.

Antirrobo

⚠ Ten en cuenta siempre que las descargas de aplicaciones hay que realizarlas desde plataformas oficiales y deben mantenerse actualizadas.

## PARA SABER MÁS

**Privacidad y seguridad en Internet:** publicación conjunta que pertenece a la Agencia Española de Protección de Datos (AEPD) y al Instituto Nacional de Ciberseguridad (INCIBE).