Universidad Veracruzana

MEDIDAS DE PROTECCIÓN EN EL USO DE DISPOSITIVOS MÓVILES

Riesgos y protección

INSTITUTO NACIONAL DE CIBERSEGURIDAD

SPANISH NATIONAL CYBERSECURITY INSTITUTE

www.incibe.es

ÍNDICE

1. MEDIDAS DE PROTECCIÓN

Para contrarrestar los riesgos del uso de dispositivos móviles, la comunidad universitaria debe aplicar las siguientes medidas de protección.

1.1 Protección antimalware y sitios web peligrosos

Las infecciones causadas por cualquier tipo de malware, siempre están presentes. Todo tipo de códigos maliciosos pueden llegar por correo electrónico y mensajería, en pendrives, a través del navegador o de aplicaciones. Además de entrenarnos para detectar enlaces y ficheros sospechosos, navegar de forma segura y descargar aplicaciones fiables, es importante disponer de **herramientas [Ref. - 1] 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 verificaremos que disponga de estas funcionalidades.

1.2 Protección contra accesos no autorizados

Para evitar que terceros sin permiso accedan a toda la información que gestiona el dispositivo es necesario implantar una serie de controles:

- **Contraseña de firmware,** si el dispositivo lo permite, sobre todo en ordenadores portátiles. De esta forma, se evita que otros usuarios arranquen el equipo desde otro disco distinto del especificado.

- **Creación de cuentas de usuario y permisos.** En los sistemas operativos como Windows, MacOS o los basados en Linux, se permite la creación de distintos usuarios, otorgándoles una serie de privilegios acordes con su perfil. Es recomendable que **cada usuario cuente con los privilegios mínimos y necesarios que le permitan desempeñar su trabajo**. Además, deberán contar con una **contraseña de acceso robusta.**

- **Bloqueo de dispositivos.** En los dispositivos basados en Android o iOS hay que establecer el **bloqueo de pantalla en el menor tiempo posible y una contraseña de desbloqueo robusta.** También pueden utilizarse métodos biométricos como la huella dactilar.

1.3 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 seguir las siguientes recomendaciones:

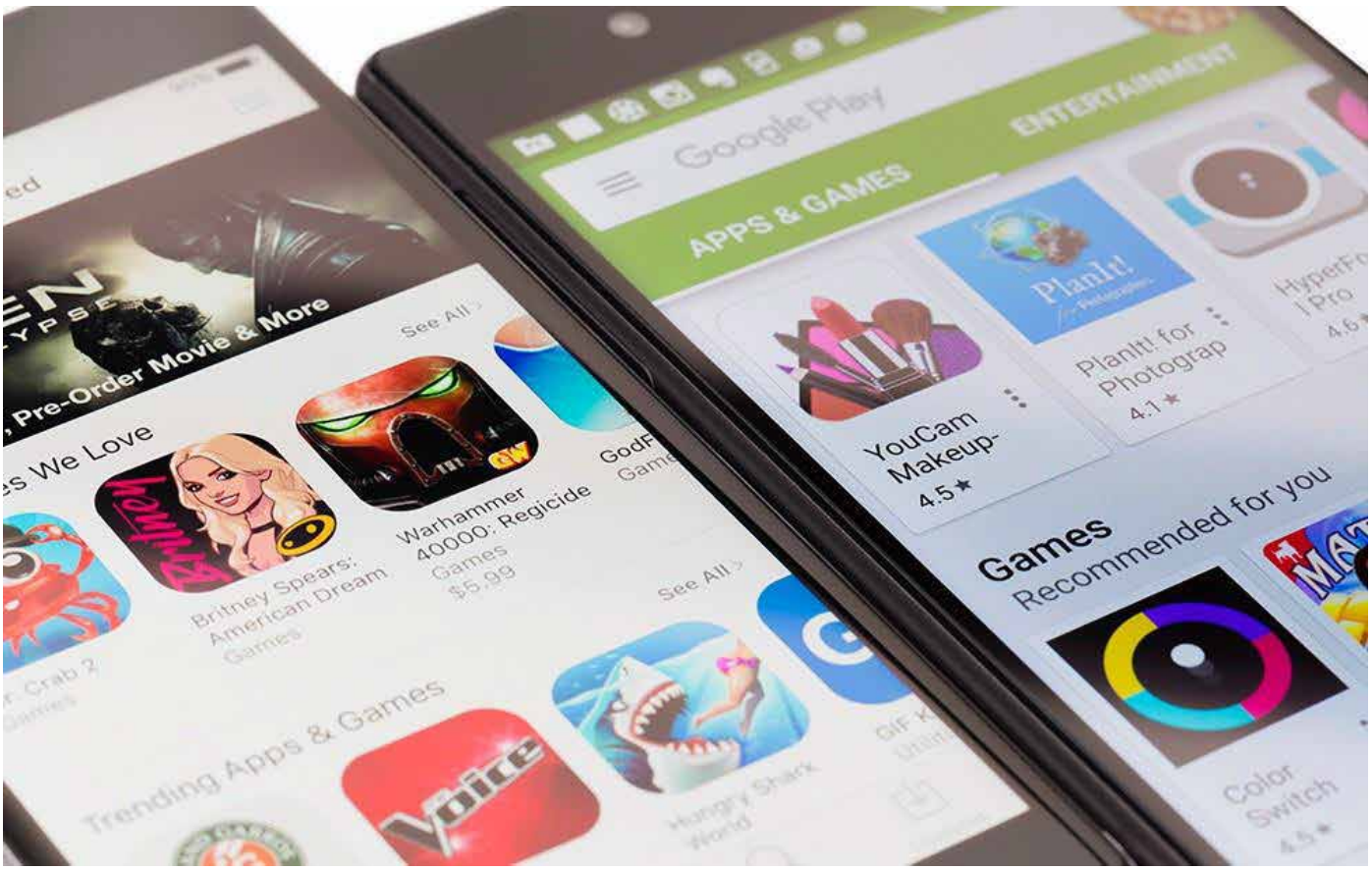
- **Activar el cifrado de la información en el dispositivo.** Todos los sistemas operativos deberán contar con herramientas de cifrado que protejan la información en ellos alojada. Los actuales sistemas operativos móviles como Android e IOS cuentan con cifrado de la información por defecto, pero los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

- **Establecer cuál será el tratamiento aceptable de la información confidencial.** En el caso del personal de administración y servicios de la universidad, investigadores y docentes, se accederá preferiblemente a la misma por medio de Internet y se evitará siempre descargar en el dispositivo.

1.4 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 descargas desde el sitio weboficial.

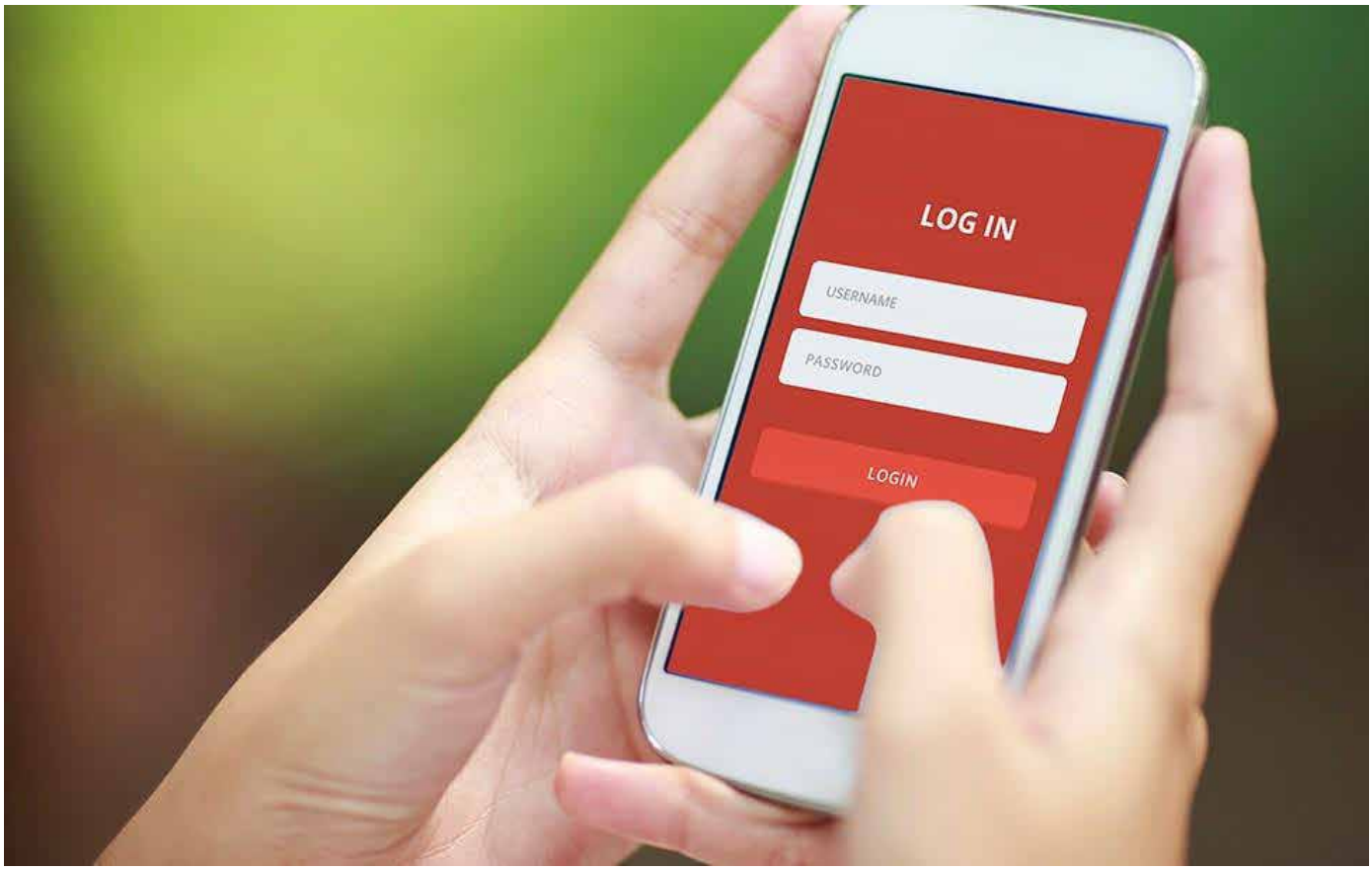
Todo el software utilizado y sistemas operativos estarán **actualizados** a la última versión disponible, además de que será siempre descargado de **fuentes legítimas** y contará con las debidas **licencias de uso.**



1.5 No recordar la contraseña

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.

En caso de utilizar múltiples servicios, con múltiples contraseñas, es recomendable utilizar un gestor de contraseñas que ayude en esa tarea.



1.6 No utilizar redes wifi inseguras

Con frecuencia nos encontramos en distintos establecimientos y servicios públicos que ofrecen conexión wifi de manera gratuita a sus clientes. A pesar del ahorro que pueda suponernos, **no es recomendable utilizar estas conexiones wifi** que nos encontramos en hoteles, restaurantes, aeropuertos, etc., ya que no conocemos su seguridad, ni su legitimidad (podrían fácilmente haberlas suplantado) y la privacidad de la información que enviamos o recibimos puede verse comprometida.

Siempre es mejor opción utilizar la conectividad móvil 4G 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.

En el caso del personal de administración y servicios, docentes e investigadores para los que sea habitual viajar por motivos de trabajo y sea necesario disponer de conectividad, se ha de **utilizar una VPN [Ref. - 2]** (red privada virtual) que cifre las conexiones extremo a extremo, para acceder a los recursos necesarios. Se evitará, en la medida de lo posible, utilizar aplicaciones de escritorio remoto para conectarse a servidores de la universidad sin VPN.

1.7 Otras medidas de protección en caso de estudio o trabajo online

En ocasiones, las tareas a realizar se tienen que trasladar al hogar **[Ref. - 3]**. Seguir manteniendo un aceptable nivel de ciberseguridad es igualmente vital, siendo necesario tomar, además del uso de aplicaciones legítimas, contraseñas, bloqueo del equipo y cifrado de información confidencial, las siguientes medidas:

- no se permitirán usos domésticos (juegos, descargas, etc.) por otros usuarios en el dispositivo utilizado como puesto de trabajo o estudio;
- se realizarán **copias de seguridad** de forma periódica;
- en caso de utilizar una **conexión wifi doméstica** que podamos configurar de forma segura **[Ref. - 4]** tendremos en cuenta:
  - utilizar cifrado WPA2 o WPA3 en caso de estar disponible y que los dispositivos sean compatibles;
  - utilizar una clave robusta;
  - desactivar la función WPS en caso de estar activa.

2. REFERENCIAS

1. INCIBE – Protege tu empresa – Blog – Descubre cómo proteger tu empresa del malware - https://www.incibe.es/protege-tu-empresa/blog/descubre-proteger-tu-empresa-del-malware

2. INCIBE – Protege tu empresa – Blog - Conéctate a tu empresa de forma segura desde cualquier sitio con una VPN - https://www.incibe.es/protege-tu-empresa/blog/conectate-tu-empresa-forma-segura-cualquier-sitio-vpn

3. INCIBE – Protege tu empresa – Blog - ¿Tu casa también es tu oficina? ¡Protégela! - https://www.incibe.es/protege-tu-empresa/blog/tu-casa-tambien-tu-oficina-protegela

4. INCIBE – Protege tu empresa – Guías - Seguridad en redes wifi: una guía de aproximación para el empresario - https://www.incibe.es/protege-tu-empresa/guias/seguridad-redes-wifi-guia-aproximacion-el-empresario