RIESGOS EN EL USO DE DISPOSITIVOS MÓVILES

Riesgos y protección

INSTITUTO NACIONAL DE CIBERSEGURIDAD
SPANISH NATIONAL CYBERSECURITY INSTITUTE
www.incibe.es

ÍNDICE

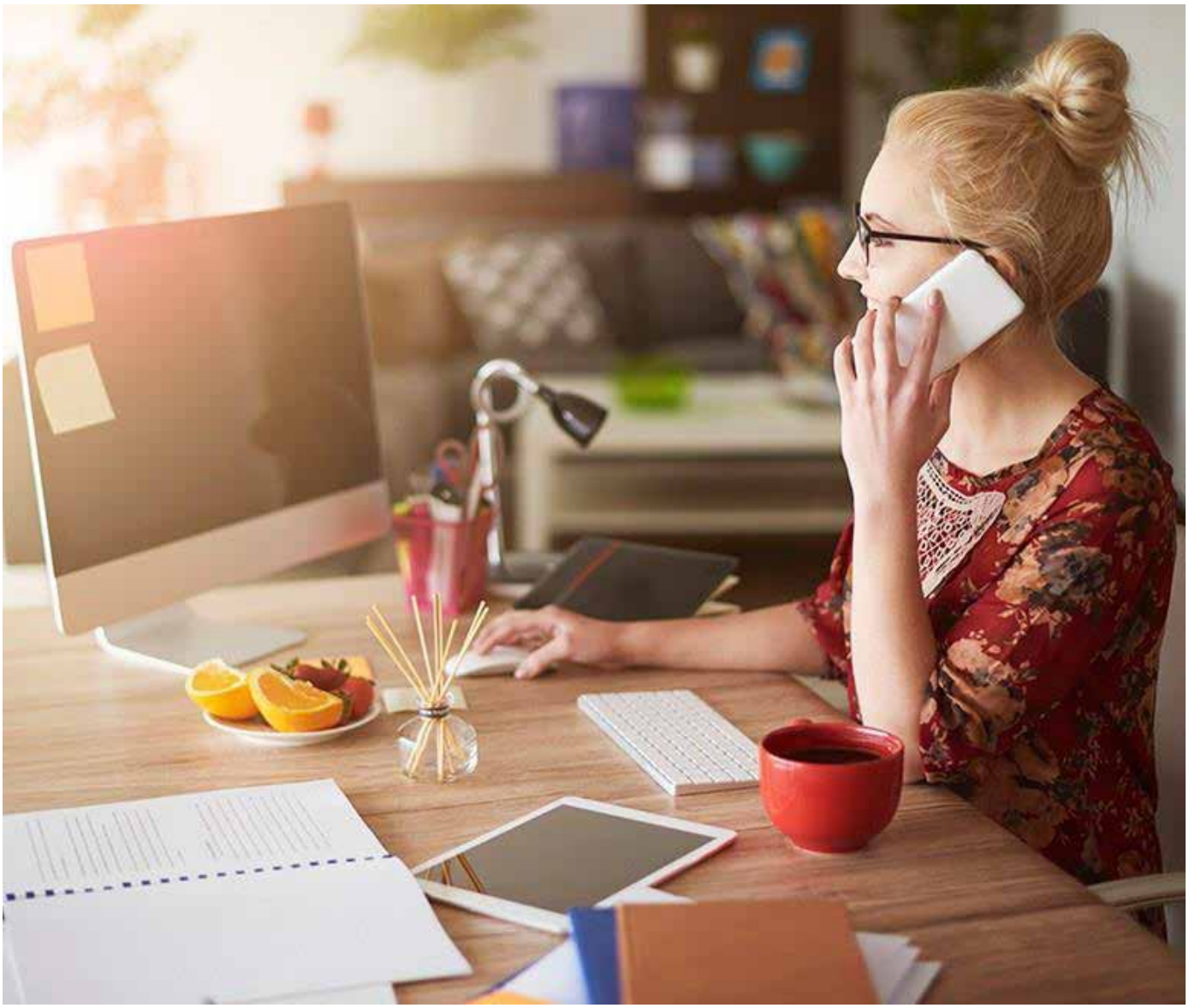
1. **Recomendaciones para el uso de dispositivos móviles** pág. 03

2. **Riesgos asociados** pág. 04

1. RECOMENDACIONES PARA EL USO DE DISPOSITIVOS MÓVILES

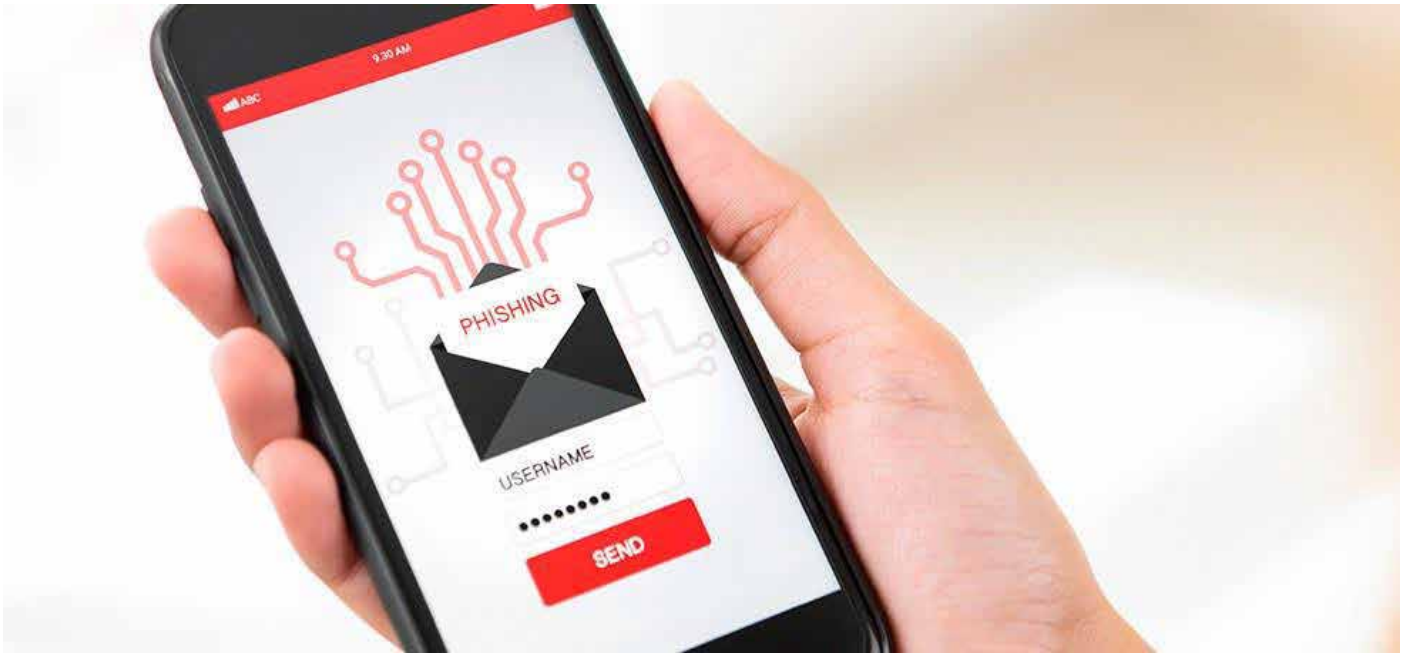
Consultar el correo, acceder a una hoja de cálculo o hacer una modificación a última hora de un documento importante, desde cualquier lugar, son solo algunas de las tareas que se pueden llevar a cabo desde los dispositivos móviles **[Ref. - 1**]. En la actualidad, estos aparatos se han convertido en herramientas imprescindibles para el trabajo o el estudio, gracias a su movilidad y su conexión a Internet.

Ordenadores portátiles, smartphones o tablets permiten a la comunidad universitaria desempeñar su trabajo o estudio en cualquier sitio, como si estuviera en las instalaciones de la universidad, lo que ha abierto un abanico nuevo de posibilidades, pero también nuevos riesgos para la universidad que los propios usuarios deben tener en cuenta.



2. RIESGOS ASOCIADOS

Los dispositivos móviles, tabletas y portátiles debido a su reducido tamaño y a la capacidad que tienen de gestionar información de la empresa, entrañan nuevos riesgos. También en el teletrabajo, además de utilizar dispositivos móviles nos conectamos desde el exterior de la red de la universidad, utilizamos servicios para compartir documentos y contamos con riesgos asociados a entornos de trabajo no tan controlados.



Estos son los principales riesgos asociados a los dispositivos móviles y al teletrabajo:

- **El robo o pérdida** de los móviles, tabletas, portátiles y dispositivos de almacenamiento como discos duros externos y pendrives. Este puede ser el riesgo más importante al que se exponen estos dispositivos debido a su tamaño y en muchos casos, a su elevado coste.

- **La infección por malware** siempre es un riesgo a tener en cuenta, pues el software malicioso puede robar información confidencial de la empresa y credenciales de acceso a diferentes recursos. A menudo descuidamos la protección antimalware en equipos pequeños.

- **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. También podemos conectarnos a redes wifi que suplantan a redes wifi lícitas.

2. RIESGOS ASOCIADOS

- **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, pudiendo así verse la información empresarial comprometida.

- Dispositivos que **no cuentan con controles de acceso robustos** que los protejan de un descuido, robo o pérdida. La ausencia de los mismos o el uso de algunos considerados débiles, como el patrón de bloqueo, son un riesgo para su seguridad.

- Tanto el **sistema operativo, como las aplicaciones desactualizadas** suponen un riesgo para la seguridad de toda la información que gestionan.

- **La modificación de los controles de seguridad impuestos por los fabricantes.** Algunos usuarios deciden rootear o hacen jailbreak a sus dispositivos lo que 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.

- **Utilización de servicios en la nube.** La utilización de servicios en la nube o cloud puede suponer un riesgo, ya que la información de la empresa será almacenada en un tercero al que hemos de trasladar nuestros requisitos de confidencialidad, integridad y privacidad. Además, existe el riesgo de que si no fuera posible conectarse a Internet (problemas en la red como congestión o caída de la misma) la información almacenada en la nube no será accesible.