BYOD o “Bring Your Own Device”, traducido a nuestro idioma oficial como el uso de tus dispositivos personales para acceder a recursos universitarios y trabajar con ellos.

Los RIESGOS más habituales son la integridad física del dispositivo (pérdida, robo, rotura) y el acceso no autorizado al mismo (físicamente o a través de virus informáticos o robo de contraseña).

Para evitar estos riesgos es recomendable adoptar unas pautas de seguridad CUANDO UTILICEMOS EL DISPOSITIVO MÓVIL.

Mantén el sistema operativo y todas tus aplicaciones SIEMPRE ACTUALIZADAS.

En un entorno BYOD debemos DIFERENCIAR claramente el correo personal del profesional.

CONFIGURA CORRECTAMENTE el dispositivo móvil y protégelo con contraseña o bloqueo. Si tienes dudas consulta a profesionales en informática para que te ayuden a hacerlo correctamente.

EVITA EL USO DE REDES WIFI PÚBLICAS, especialmente si vas a manejar información sensible, acceder a bancos o a la red institucional de la UNED.

CIFRAR LOS DISPOSITIVOS MÓVILES reducirá el impacto en el caso de que se produzca una pérdida o un robo. Además, esta medida ayuda a proteger tu información personal.

Haz uso del modo NAVEGACIÓN DE INCOGNITO que incluye la mayoría de los navegadores.