RECUERDA: KIT DE CONCIENCIACIÓN

BYOD: "BRING YOUR OWN DEVICE"

- Deshabilita la sincronización de tu dispositivo con "la nube" cuando manejes información sensible.
- Nunca permitas que el navegador guarde o recuerde tus credenciales de acceso corporativo. Desactiva también la opción de auto-completado de formularios.
- Utiliza una conexión 3G o 4G para conectarte a tu red corporativa en lugar de WiFi y si está habilitada utiliza la VPN.
- Protege tu información y la de la universidad estableciendo en tu dispositivo móvil una clave de acceso y la opción de bloqueo automático.
- Debemos diferenciar las contraseñas de acceso al entorno personal del profesional.
- Utiliza sólo las tiendas oficiales para descargar las aplicaciones que quieras instalar en tu móvil. No utilices aplicaciones legítimas en ninguno de tus dispositivos.
- Nunca dejes tus equipos desatendidos en lugares públicos o en tu vehículo. Ponlos también a salvo de accidentes domésticos cuando no los estés utilizando.

CONTÁCTANOS

Twitter
@unisevilla

YouTube
UniversidaddeSevilla

Facebook
UniversidaddeSevillaoficial

Linkedin
universidad-de-sevilla

Instagram
@unisevilla

Producto diseñado y desarrollado por INCIBE.
Adaptación a universidades realizada por MetaRed.

INSTITUTO NACIONAL DE CIBERSEGURIDAD

SPANISH NATIONAL CYBERSECURITY INSTITUTE

www.incibe.es

Kit de Concienciación

BYOD "BRING YOR OWN DEVICE"

Universidad de Sevilla

crue Universidades Españolas

BYOD o "Bring Your Own Device", es una política que se puede aplicar en tu universidad, que permite que los empleados hagan uso de sus dispositivos personales para acceder a recursos corporativos.

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

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

El CIFRADO DE LAS CONEXIONES para el acceso a la información institucional es una de las medidas más eficaces a la hora de proteger la información cuando los dispositivos se utilizan fuera de la red corporativa.

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

CONFIGURA CORRECTAMENTE el dispositivo móvil y protégelo de forma adecuada. El centro de atención al usuario del área TIC de tu universidad te puede ayudar a hacerlo correctamente.

CONOCE Y CUMPLE LA POLÍTICA de tu universidad en cuanto al uso de BYOD.

EVITA EL USO DE REDES WIFI PÚBLICAS, especialmente si vas a manejar información sensible, acceder a cuentas bancarias, a la red institucional, etc.

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.

Mantén el sistema operativo y todas tus aplicaciones SIEMPRE ACTUALIZADAS.

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