RECUERDA: KIT DE CONCIENCIACIÓN
DISPOSITIVOS MÓVILES

- La información que guardamos en nuestros dispositivos móviles es valiosa, protégela.
- Un dispositivo móvil se puede perder, puede ser robado, roto, destruido o averiarse, más vale prevenir.
- Aplica medidas para evitar accesos no autorizados a tu información.
- Cifra tus dispositivos móviles.
- Evita el uso de WiFis públicas cuando trates información sensible.
- Si utilizas BYOD configura correctamente los dispositivos móviles.
- El departamento de seguridad o sistemas debe configurar la seguridad de los dispositivos móviles antes de su entrega.
- Desactiva las funciones de geoposicionamiento cuando sea posible.

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

incibe_
www.incibe.es

Kit de Concienciación

DISPOSITIVOS MÓVILES

UNIVERSIDAD DE SEVILLA

crue Universidades Españolas

LOS DISPOSITIVOS MÓVILES más utilizados son los ordenadores portátiles, los smartphones y las tablets.

LOS RIESGOS más habituales para estos dispositivos son la pérdida, el robo, la rotura, destrucción o avería.

Para evitar estos riesgos es recomendable implantar las LAS MEDIDAS DE SEGURIDAD pertinentes.

Los dispositivos móviles (portátiles, tablets,...) permiten habilitar y deshabilitar las funciones de GEOPOSICIONAMIENTO. Su objetivo es obtener la ubicación geográfica del dispositivo.

Es recomendable DESACTIVAR las funciones de GEOPOSICIONAMIENTO de los dispositivos móviles, para evitar difundir más información de la necesaria.

BYOD o Bring Your Own Device, es una tendencia que se basa en que los empleados hagan uso de sus dispositivos personales en el entorno de trabajo.

Es necesario que los dispositivos BYOD estén sujetos a las mismas condiciones de seguridad que los dispositivos corporativos o incluso a medidas de seguridad adicionales.

WiFi NO es recomendable hacer uso de redes WIFI PÚBLICAS si vamos a tratar información sensible, acceder a cuentas bancarias, a la red institucional, etc.

VPN Si necesitamos conectividad fuera de nuestras oficinas, es conveniente usar ALTERNATIVAS DE CONEXIÓN a redes WiFi públicas como son el 3G o el uso de VPNs.

Es necesario establecer un PROCEDIMIENTO PARA SECURIZAR los nuevos dispositivos móviles, antes de su uso.

Es recomendable que el departamento de seguridad o sistemas lleve a cabo la correcta CONFIGURACIÓN DE SEGURIDAD de los dispositivos móviles antes de entregarlos para su uso.

EL CIFRADO de los dispositivos móviles es una de las medidas más eficaces a la hora de proteger la información cuando éstos se usan fuera de nuestra universidad. De este modo, se reduce el impacto por pérdida o robo.