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 tu empresa 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 ilegítimas** en ninguno de tus dispositivos.
- Nunca dejes tus **equipos desatendidos** en lugares públicos o en tu vehículo. Ponlos también a salvo de accidentes.

CONTÁCTANOS

info@incibe.es

Twitter
@incibe
@certsi_
@osiseguridad

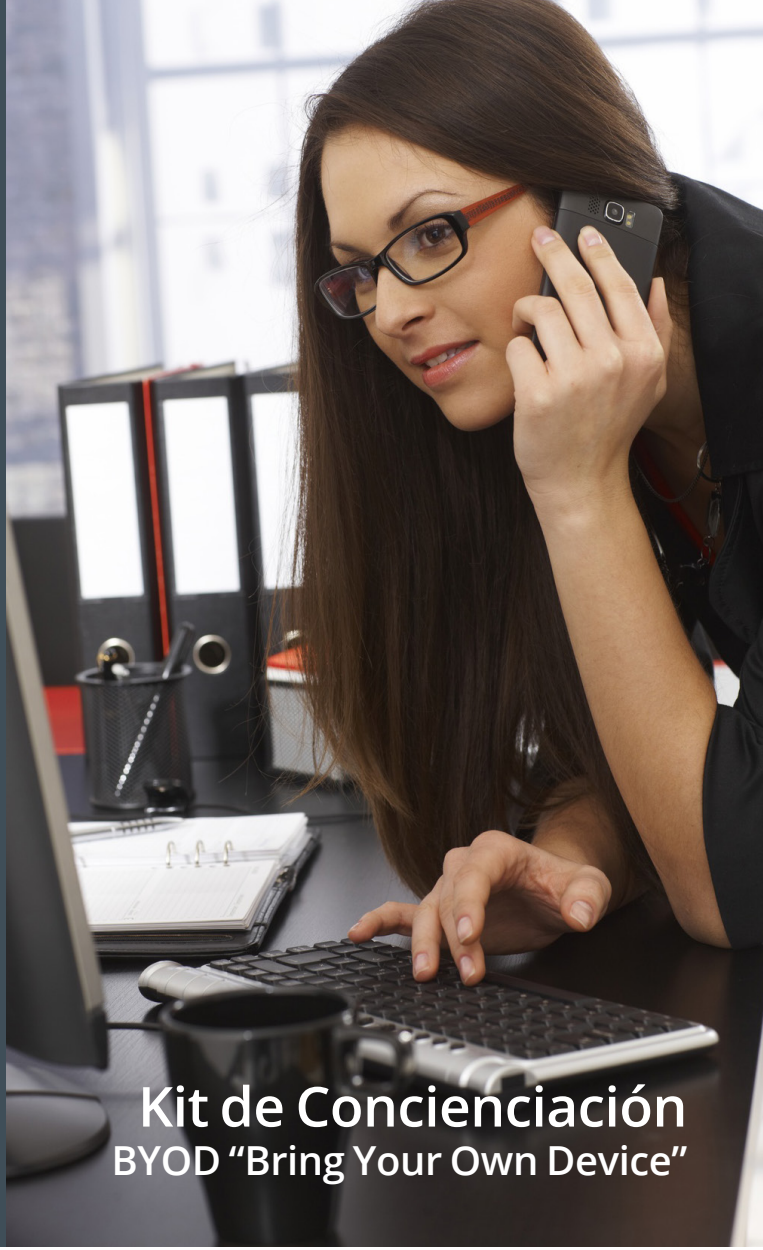
YouTube
Intecocert
OSIseguridad

Facebook
Osiseguridad

Linkedin
Incibe-sa

Google+
Oficina de Seguridad del Internauta

Tuenti
Oficina de Seguridad del Internauta



Kit de Concienciación
BYOD "Bring Your Own Device"

INSTITUTO NACIONAL DE CIBERSEGURIDAD

www.incibe.es

Av. José Aguado 41 / 24005 León
T. (+34) 987 877 189 / F. (+34) 987 261 016

INSTITUTO NACIONAL DE CIBERSEGURIDAD

SPANISH NATIONAL CYBERSECURITY INSTITUTE

incibe_

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

BYOD o "Bring Your Own Device", es una política de empresa que permite que los empleados hagan uso de sus dispositivos personales para acceder a recursos corporativos.

Los **RIESGOS** más habituales para tu empresa 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.**

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

CONFIGURA CORRECTAMENTE el dispositivo móvil y protégelo de forma adecuada. El departamento de informática te puede ayudar a hacerlo correctamente.

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

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

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.

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

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

Mantén el sistema operativo y todas tus aplicaciones **SIEMPRE ACTUALIZADAS.**