

RECUERDA: KIT DE CONCIENCIACIÓN LAS REDES SOCIALES

- Una broma o comentario inadecuado podría afectarte personal y profesionalmente.
- Configura tu privacidad con las opciones que te ofrece la red social. Elige el nivel apropiado de privacidad.
- No reutilices contraseñas de acceso a los recursos corporativos para acceder a las redes sociales.
- Protege tu información personal.



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



 **crue**
Universidades
Españolas

Kit de Concienciación

LAS REDES SOCIALES



Actualmente, las redes sociales se han convertido en una herramienta muy importante para la sociedad, y la comunidad universitaria no iba a ser menos.

Mediante las redes sociales los estudiantes, docentes, investigadores o personal de administración y servicios pueden realizar contactos, compartir opiniones, estudios, proyectos, eventos, etc. tanto de su vida personal como profesional.



privacidad Ten cuidado al emitir juicios de valor a nivel personal, estos pueden afectar a tu reputación.



Para evitar estos riesgos es recomendable adoptar una buenas prácticas en **EL USO DE LAS REDES SOCIALES**.



Evita **PUBLICAR INFORMACIÓN** que pueda comprometer tu seguridad y privacidad.



Configura la privacidad de tu perfil, utiliza **CONTRASEÑAS ROBUSTAS**, controla los permisos que les das a las aplicaciones que acceden a tus perfiles en redes sociales.



No utilices el **CORREO DE LA UNIVERSIDAD** para unirte a una red social. Usa siempre en estos casos tu email personal.



Ten en cuenta la información que revelas sobre tu **LUGAR DE TRABAJO**. Cuidado con las fotos, direcciones, etc.



Atento a las **CAMPAÑAS DE FRAUDE** que se hacen a través de las redes sociales, como por ejemplo malware o phishing.