

RECUERDA: KIT DE CONCIENCIACIÓN LAS REDES SOCIALES

- Un comentario inadecuado podría afectar a la reputación de la Universidad
- Configura tu privacidad con las opciones que te ofrece la red social. Elige el nivel apropiado de privacidad.
- No publiques el nombre de la universidad si no estás autorizado para ello y desactiva las funciones de geoposicionamiento cuando sea posible.
- No reutilices contraseñas de acceso a los recursos corporativos para acceder a las redes sociales.
- No emitas valoraciones personales en nombre de la universidad.
- Protege tu información personal y la de la universidad.



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.



Las universidades se encuentran representadas en las redes sociales tanto a través de los perfiles profesionales de las personas que trabajan en ellas como a través de páginas corporativas.



Ten cuidado al emitir juicios de valor a nivel personal sobre temas que atañen a la universidad. Estos pueden afectar no solo a tu prestigio sino también al de la universidad.



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



CONOCE Y CUMPLE LA POLÍTICA de la universidad en cuanto al uso de la redes sociales.



Evita **PUBLICAR INFORMACIÓN** corporativa que pueda comprometer la seguridad de la universidad.



Los **RIESGOS** derivados del uso de las redes sociales en el entorno de la universidad suelen ser, entre otros, juicios de valor por parte del responsable de las redes, utilizar un tono elevado que genere polémica o revelar información confidencial o privada.



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



Prestar mucha atención a las **CAMPAÑAS DE FRAUDE** que se realizan a través de las redes sociales, como pueden ser suplantaciones, malware o phishing.



OTROS RIESGOS relacionados con la privacidad y la seguridad son utilizar contraseñas débiles, permitir que cualquiera pueda publicar en las redes de la universidad, o los permisos que se le dan a las aplicaciones que acceden a las redes sociales.