

RECUERDA: KIT DE CONCIENCIACIÓN LA INFORMACIÓN

- ❑ Usa una política need-to-know, el usuario sólo accede a la información que necesita para su trabajo.
- ❑ Aplica medidas para evitar accesos no autorizados y detectar intentos de acceso.
- ❑ Cifra la información confidencial.
- ❑ Haz copias de seguridad de la información importante, confidencial y sensible.
- ❑ Comprueba que tus copias de seguridad funcionan correctamente.
- ❑ Clasifica la información y protégela en consecuencia.
- ❑ Elimina los metadatos (información sensible oculta en los ficheros), antes de enviar los ficheros.



UNIVERSIDAD DE GRANADA

- ➔ protecciondedatos@ugr.es
958 240874
- ➔ seguridadinformacion@ugr.es
958 241408

CONTÁCTANOS

- ✉ ciberseguridad@metared.org
- 🐦 Twitter
[@infometared](https://twitter.com/infometared)
- 📘 Facebook
[@MetaRedGlobal](https://www.facebook.com/MetaRedGlobal)
- in LinkedIn
<https://www.linkedin.com/in/metared/>

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



**UNIVERSIDAD
DE GRANADA**

Kit de Concienciación

LA INFORMACIÓN





INFORMACIÓN CONFIDENCIAL

es toda aquella información que requiera aplicar medidas de seguridad para evitar su difusión. No importa el soporte, el tipo de información o si se ha comunicado verbalmente.



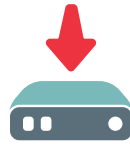
LAS MEDIDAS BÁSICAS

que debemos aplicar son: la firma de acuerdos de confidencialidad, el acceso restringido a la información (política need-to-know), detectar y evitar accesos e intentos de acceso no autorizados así como cifrar la información cuando sea necesario.



EL CIFRADO

de la información es una de las medidas más eficaces a la hora de proteger la información. Debemos cifrar la información vital para nuestra universidad, los datos personales de nivel alto y cualquier información sensible que vayamos a enviar.



LAS COPIAS DE SEGURIDAD

garantizan la continuidad de nuestra universidad. Su función es la de recuperar nuestros datos en caso de pérdida, fallo o contingencia general. Es fundamental que decidamos aspectos como la frecuencia, el tipo de copia o el soporte donde se realizan. También se debe comprobar cada cierto tiempo que funcionan correctamente.



Es necesario establecer una **CLASIFICACIÓN DE LA INFORMACIÓN** y según los niveles definidos establezcamos las medidas de seguridad oportunas para su correcto tratamiento.



ELIMINAR LOS METADATOS

o información sensible oculta en los ficheros digitales (como nombre de usuario del sistema, histórico de correcciones,...) que vayamos a enviar, ya que podemos estar proporcionando información valiosa sobre la organización sin saberlo.