

RECUERDA: KIT DE CONCIENCIACIÓN DECÁLOGO SOBRE LOS PUNTOS CLAVE

- ❑ No utilices tus credenciales de acceso a servicios de la universidad en aplicaciones de uso personal.
- ❑ No pinches en enlaces (links) sospechosos. Mejor escribe la dirección en la barra del navegador.
- ❑ Protege la información impresa utilizando mobiliario con cierres, cajas fuertes o armarios ignífugos.
- ❑ Procura no transportar información sensible en dispositivos extraíbles. Si lo haces, cifra la información.
- ❑ Aprende a detectar los ataques de ingeniería social y como defenderte. Avisa si ves un comportamiento anómalo.
- ❑ Bloquea la sesión de tu equipo cuando abandones tu puesto de trabajo.
- ❑ No modifiques la configuración de tus dispositivos móviles ni instales aplicaciones no autorizadas.
- ❑ Evita el uso de equipos no corporativos para acceder a servicios de la universidad. Si accedes al correo corporativo desde tu equipo personal, no descargues ficheros al equipo.
- ❑ Destruye la información sensible en formato papel. No te limites a tirarla a la papelera y evita una fuga de información.
- ❑ Sé cuidadoso con el uso del correo electrónico. Evita los correos en cadena.



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)
- 🌐 LinkedIn
<https://www.linkedin.com/in/metared/>

Producto diseñado y desarrollado por INCIBE.
Adaptación a universidades realizada por MetaRed.

DECÁLOGO SOBRE LOS PUNTOS CLAVE





Debemos conocer y concienciarnos de los **PUNTOS MÁS IMPORTANTES O CLAVE** de seguridad e implantar las **MEDIDAS OPORTUNAS DE SEGURIDAD** para la adecuada protección de la información a la hora de desempeñar nuestra actividad profesional.



Debemos proteger nuestro **PUESTO DE TRABAJO** y mantener la mesa "limpia" de papeles que contengan información sensible.



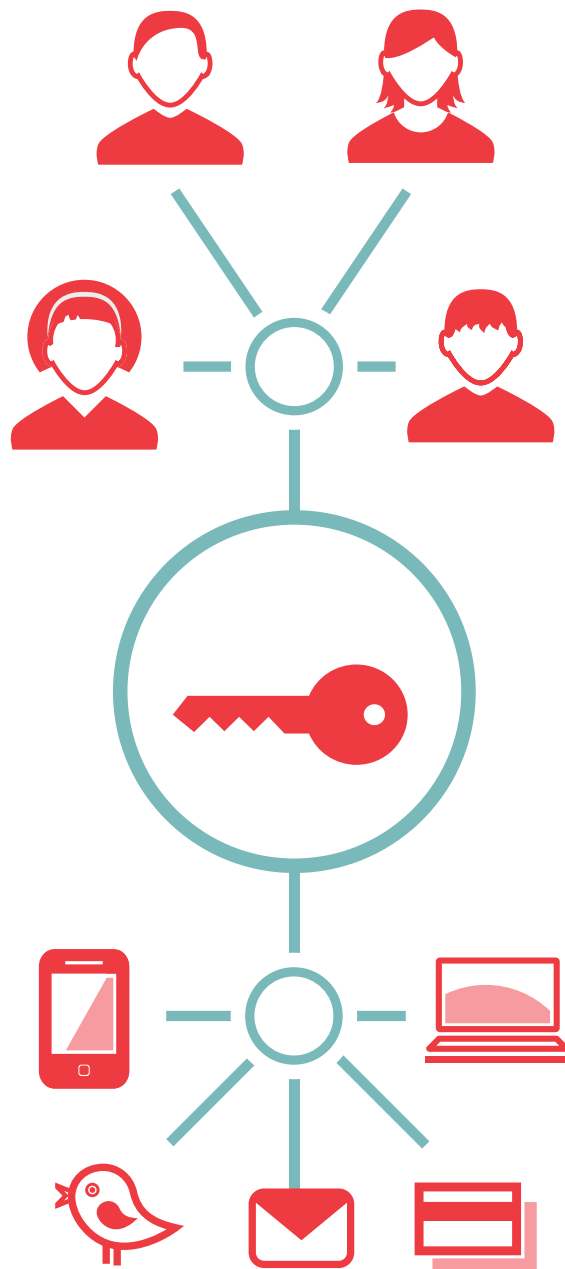
Es recomendable establecer en tu **DISPOSITIVO MÓVIL** una clave de acceso y la opción de bloqueo automático.



No hagas uso de **EQUIPOS NO INSTITUCIONALES**. Si es necesario, no manejes información institucional en este tipo de equipos.



Evita las **FUGAS DE INFORMACIÓN**. No mantengamos conversaciones confidenciales en lugares donde puedan ser oídas por terceros.



LAS CONTRASEÑAS deben ser secretas y únicas, no debemos anotarlas, compartirlas o reutilizarlas.



Se debe realizar una **NAVEGACIÓN SEGURA** y evitar acceder a páginas web no confiables.



Utiliza el **CORREO ELECTRÓNICO** de forma segura y elimina o informa a tu departamento de informática todo correo sospechoso que recibas.



Protege **LA INFORMACIÓN** y realiza copias de seguridad de la información sensible que solo esté en nuestro equipo.



Cuando **VIAJES**, no mandes información sensible a través de redes WIFI no confiables.



TODOS SOMOS SEGURIDAD. Debemos avisar al departamento de seguridad si detectamos cualquier actividad sospechosa.