



- **Identificación:** capacidad de identificar, de manera exclusiva, a un usuario de un sistema o servicio que se está ejecutando.
- **Autenticación:** capacidad de demostrar que ese usuario que se ha identificado, es realmente quien dice ser.
- **Autorización:** validación de los permisos de acceso por parte de un usuario o servicio autenticado.

MÉTODOS DE AUTENTICACIÓN:

Autenticación por conocimientos

Este método está basado en la información que solo es conocida por el usuario, como una contraseña o código.



ALGO QUE EL USUARIO SABE

Autenticación por pertenencia

En este caso, se centra en un objeto que posee el usuario, como una tarjeta identificativa con la que acceder a las instalaciones de la organización.



ALGO QUE EL USUARIO TIENE

Autenticación por características

Este método hace referencia a alguna característica física del usuario o datos biométricos, por ejemplo, las huellas dactilares o la retina.



ALGO QUE EL USUARIO ES

TIPOS DE AUTENTICACIÓN QUE INCREMENTAN LA SEGURIDAD DE LOS SISTEMAS O DISPOSITIVOS:

Autenticación de factor único

Permite la autenticación a través de la comprobación de uno de los factores de autenticación mencionados.



Se solicita nombre de usuario y contraseña para acceder.

Autenticación de doble factor (2FA)

Se basa en una confirmación extra para el acceso, es decir, requiere dos factores diferentes.



Se introduce una primera clave y se recibe un SMS en el teléfono móvil que se debe incluir como segunda clave y confirmar la operación.

Autenticación multifactor (MFA)

Es aquella que utiliza más de dos factores de autenticación.



Solicitud de contraseña, recepción de un código a través del teléfono móvil y uso de huella dactilar.



Convendrá aplicar más o menos factores de autenticación en función de la importancia de lo que se quiera proteger o emplear los mismos factores pero más seguros.