



## 2WIN-S y 2WIN-S Plus cumplen con el GDPR

En Adaptica nos preocupan los datos. Protegemos sus datos y los de sus clientes.

En este documento se explican las características de privacidad y seguridad de 2WIN y 2WIN-S Plus y se dan pistas sobre cómo mejorar aún más la seguridad de los datos.

### Características de seguridad de 2WIN-S y 2WIN-S Plus

2WIN-S y 2WIN-S Plus están compuestos por una cámara de cribado visual 2WIN, un tubo Kaleidos y una tableta de control que ejecuta la aplicación KALEIDOS BT. Estas son las características y especificaciones relativas a la seguridad de los datos almacenados en los dos dispositivos.

- El 2WIN-S sólo realiza exámenes anónimos, por lo que no se almacenan datos personales en el dispositivo.
- En la KALEIDOS App BT es posible insertar datos del paciente (disponible a partir de la versión de software 5.4). Estos datos no se envían al 2WIN-S y se mantienen dentro de la tableta de control.
- KALEIDOS App BT sólo funcionará si se configura un bloqueo de seguridad en la tableta de control. La aplicación avisará al usuario si el bloqueo de seguridad no está configurado y no se iniciará hasta que se configure.
- La aplicación AI (disponible a partir de la versión de software 5.5.0) sólo envía y almacena datos anónimos y la cantidad mínima necesaria para el servicio, si es necesario.
- La integración del EMR (disponible a partir de la versión de software 5.5.0) requiere que el usuario configure una carpeta compartida. Esto debe hacerse con el protocolo samba y requiere que se establezca una contraseña en la carpeta compartida.
- En la carpeta compartida sólo se guarda un examen a la vez, para evitar múltiples exámenes que no estén bajo el control directo de la aplicación.

### Consejos para mejorar la seguridad

Para mejorar la seguridad de los datos se recomiendan encarecidamente las siguientes acciones.

1. Encripte su tableta de control con una identificación o contraseña segura.  
2WIN-S Plus viene con una consola remota (tableta) dedicada, que ya está encriptada con una contraseña por defecto. Sin embargo, nos gustaría que estableciera su propia contraseña, para que sólo usted pueda acceder a sus datos. En caso de que el dispositivo sea robado, esto evitaría que extraños accedan a los datos que hay dentro.  
Elige un bloqueo de pantalla de seguridad adecuado, como un ID con al menos 6 números o una contraseña de al menos 8 caracteres que incluya mayúsculas, números y símbolos.
2. El mismo consejo para la contraseña es válido para proteger la carpeta compartida del EMR.
3. Para proteger la carpeta compartida del EMR, actualice regularmente el PC o el servidor desde el que se configura la carpeta compartida con los últimos parches de seguridad del sistema operativo.