


TELETRABAJO



El teletrabajo conlleva el riesgo de trabajar en lugares que no disponen de las medidas de seguridad físicas y lógicas implementadas en los centros de trabajo. Se deben adoptar medidas de seguridad complementarias para garantizar un adecuado nivel de protección de la información.


BUENAS PRÁCTICAS


👍 Asegúrate que el **sistema operativo** de tu dispositivo está **actualizado**.


👍 Debes disponer de un **antivirus actualizado** en tus dispositivos. 

👍 Comprueba los **programas** instalados y que estén **actualizados**.




👍 **Protege la red WiFi de tu casa.** Cambia el nombre y contraseña de tu red WiFi y la contraseña de la página de configuración del router. 


👍 Crea contraseñas complejas y exclusivas para prevenir la filtración de datos. 


👍 Realiza **conexiones seguras** siempre a través de la **VPN**. 


👍 **No uses redes wifi públicas para teletrabajar.** 


👍 **Respetar el deber de secreto profesional.** Evita el acceso a información corporativa por familiares.


👍 **Bloquea** la pantalla del dispositivo si te ausentas o **apágalo** si vas a dejar de usarlo. 

👍 No copies información corporativa a los servicios en la nube (Google Drive, Dropbox...) 

👍 **Cuidado** con la copia de **información corporativa** al **equipo personal**. 

👍 Revisa las pantallas y contenidos que compartes en sesiones de videoconferencia. 

👍 Comprueba donde imprimes documentación sensible, no estés en la oficina. 

👍 Recuerda aplicar las buenas prácticas...
- *Correo electrónico*
- *Phishing*
- *Malware* 

👍 Para cualquier incidencia, contacta con tu centro de atención a usuarios, preferentemente a través de **SIGUE**.