Recomendaciones sobre el uso de dispositivos personales para la función docente

El uso de dispositivos personales y privados para fines educativos tiene que tener presente la **protección de sus propios dispositivos,** como medidas destinadas a proteger los **datos personales** y **los del centro educativo**, para ello algunas recomendaciones previas serían, por ejemplo:

- **Configurar** correctamente los **parámetros de seguridad** del dispositivo.
- Mantener **actualizado** el dispositivo y sus aplicaciones.
- Activar el **cifrado de datos** en el dispositivo.
- No instalar aplicaciones que no sean de confianza y ser restrictivos a la hora de dar permisos para las instaladas en el dispositivo, pues pueden incluir malware y, por tanto, hacer vulnerable el dispositivo e incluso las redes a las que puede conectarse.
- Establecer mecanismos de **bloqueo automático** con contraseña, incluso con borrado automático de la información tras un número de intentos fallidos.
- Activar el bloqueo de pantalla automático tras un breve periodo de inactividad. El desbloqueo debe realizarse mediante contraseña o patrón de desbloqueo.
- Activar un sistema de **localización por GPS** para casos de pérdida.
- No activar el recuerdo de contraseña para los sistemas corporativos de la organización educativa.

Imagen de DCStudio en Freepik

Por otro lado debemos **diferenciar** el almacenamiento de **datos de trabajo con respecto a los datos privados**. Debe evitarse el almacenamiento de datos personales corporativos en dispositivos personales o en nubes no corporativas y viceversa. Por lo tanto, si se utiliza un dispositivo electrónico personal y es necesario consultar un dato personal en la nube corporativa, debe evitarse almacenar ese dato en el dispositivo o que se guarde una copia en otra nube privada no corporativa. En caso de que no se siga esta recomendación, el responsable deberá evaluar los riesgos que conlleva este almacenamiento y determinar las medidas organizativas y técnicas a adoptar, así como formar e informar convenientemente a los usuarios finales que traten esos datos personales, en especial si son de menores de edad.

Debemos **consultar a los responsables de las redes del centro**, si podemos conectarnos a las mismas y qué protocolo hay establecido (con IP estática, IP dinámica, posibles contraseñas,...). Si nos conectamos a las redes Wifi públicas o Wifi privadas: valorar si el acceso a las mismas no compromete la privacidad y seguridad de nuestras funciones docentes.

Podríamos empezar a elaborar, una plantilla para el centro, de la siguiente manera:

RECOMENDACIONES SOBRE EL USO DE DISPOSITIVOS PERSONALES

- Configurar correctamente los parámetros de seguridad del dispositivo.
- Establecer mecanismos de bloqueo automático con contraseña.
- Diferenciar el almacenamiento de datos de trabajo con respecto a los datos privados.
- …

Revision #17
Created 10 January 2023 23:05:24 by Javier Gerico
Updated 20 March 2023 13:02:04 by María Esther Arilla Luna