Recomendaciones para la utilización de dispositivos móviles personales para uso profesional (BYOD)

El término **BYOD** hace alusión a la posibilidad de que los empleados incorporen sus dispositivos móviles a la red corporativa, para poder acceder desde su propia casa, la oficina o cualquier otro lugar, aceptando que la utilización de dicho dispositivo pueda emplearse para tareas corporativas como para personales.

Si bien, se trata de un fenómeno frecuente que proporciona numerosas ventajas a la entidad, también posee de manera intrínseca una serie de riesgos que debemos intentar aminorar, como por ejemplo, instalación de aplicaciones que puedan comprometer la confidencialidad de los datos o la propia coexistencia de datos personales y corporativos.

Los riesgos que soporta este sistema de trabajo:

- **Posible pérdida, robo o destrucción del dispositivo:** al ser dispositivos portátiles de pequeño tamaño y habitual uso, la probabilidad de su extravío se incrementa.
- **Robo de credenciales**: ocasionado por cualquier descuido en materia de contraseñas o controles de acceso.
- **Pérdida de información:** si el dispositivo solo cuenta con una protección adecuada a nivel privado, la configuración existente no abarca en algunas ocasiones la seguridad que se debe pretender en el entorno corporativo.
- **Conexión a redes inseguras:** es frecuente la necesidad que surge en entornos ajenos a la oficina o al domicilio, de conectarse a una red para poder trabajar. Las redes abiertas de cortesía que existen en bares, restaurantes, hoteles, etc. son poco seguras, empleadas frecuentemente por ciberdelincuentes y por ello debemos ser cautos a la hora de conectarnos a ese tipo de conexiones.
- **Usuarios:** una gestión descuidada de un dispositivo personal empleado para uso profesional puede ocasionar enormes riesgos, por ello, los empleados deben estar concienciados en materia de ciberseguridad, indicando al responsable cualquier incidente o posible vulneración de seguridad que pueda tener lugar.

Para minimizar dichos riesgos deben tomarse las siguientes recomendaciones:

- **Instalación de aplicaciones seguras**: es importante que el usuario descargue únicamente aplicaciones que sean seguras, y se lleve por el mismo una correcta admisibilidad de los permisos que requieren. Para ello es recomendable leer las condiciones de uso e instalación, así como su descarga únicamente de markets oficiales (Play Store, App Store, etc.)
- **Almacenamiento de datos en la nube:** si los datos corporativos se encuentran almacenados en la nube, su acceso por parte del empleado fuera de la oficina

será más sencillo y más seguro. Si bien, el usuario sólo deberá guardar en la nube los documentos autorizados por parte del responsable.

- **Copias de seguridad:** no debemos olvidarnos de la existencia de estos dispositivos a la hora de gestionar nuestra política de copias de seguridad. Por ello, es recomendable que las copias de seguridad se realicen automáticamente y se almacenen fuera del dispositivo, como podría haberse a través de un backup online en la nube.
- **Cifrado de dispositivos:** para evitar el impacto que tendría un robo o extravío del dispositivo, se debe utilizar un sistema de información cifrada.
- **Medidas técnicas de configuración:** se debe contar con sistemas de autenticación robustos (contraseñas de dificultad alta), instalación y configuración de un antivirus, configuración en actualizaciones del software, cifrado de extremo a extremo en comunicaciones y datos, así como el no permitir que el dispositivo recuerde las contraseñas.
- **Localización remota del dispositivo:** que pueda ser utilizada en el caso de que se sufra una pérdida o robo del mismo, permitiendo conocer la localización del terminal, su bloqueo remoto, así como el borrado remoto de los datos y el seguimiento de la actividad realizada con el mismo. Ahora bien, este tipo de facultades sólo deberán ser utilizadas en caso justificado, ante una pérdida o robo del dispositivo.
- **Medidas de protección ante redes externas:** evitar conectarse a redes wifi públicas o gratuitas, utilizar canales cifrados de comunicación VPN, desconectar la búsqueda de conexiones wifi cuando no las estemos empleando, desactivar la conexión automática a redes, y preferiblemente, hacer uso del 3G o 4G antes que de conexiones wifi inseguras.
- **Política de uso:** restringir la utilización de dispositivos ajenos no autorizados por el responsable (locutorios, puestos de internet compartido en hoteles, etc.), solo emplear aquellos dispositivos que cuenten con los requisitos de seguridad necesarios, crear una base de datos que almacene los datos de carácter corporativo generados en los dispositivos móviles, restringir en medida de lo posible la instalación de aplicaciones de terceros.
- **Revisión del sistema de seguridad de los dispositivos por el responsable:** el responsable estará facultado, y deberá realizar revisiones del sistema de seguridad en el caso de que exista cualquier sospecha de vulnerabilidad en los dispositivos. Para ello, de manera previa deberá solicitar el consentimiento expreso por parte del trabajador, y limitar su acceso al dispositivo a las medidas de seguridad que el mismo dispone.

Ecomputer, S.L. recomienda a Gestión de Residuos Huesca, S.A.U, que tenga en cuenta las siguientes recomendaciones para una utilización segura de los dispositivos personales para su uso corporativo.