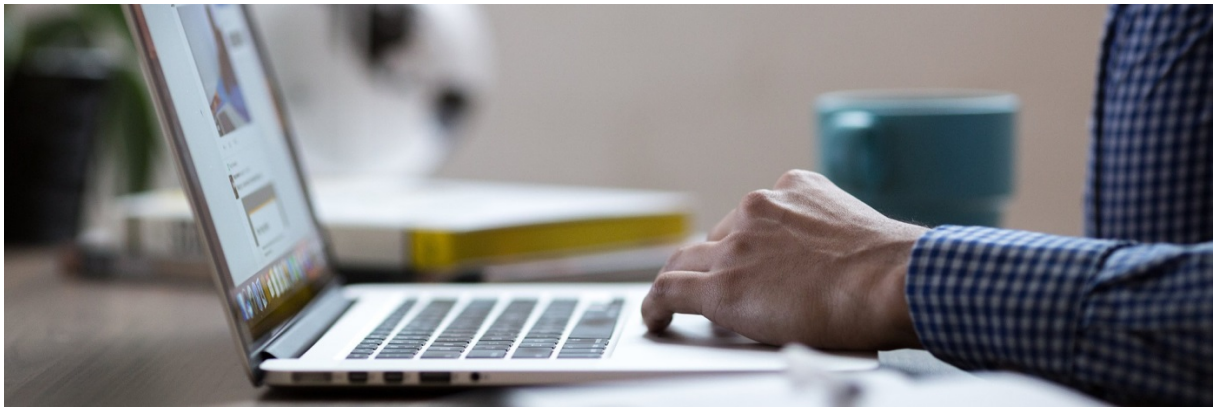

¿Cómo podemos proteger nuestros datos personales en situaciones de movilidad y teletrabajo?

La Unidad de Evaluación y Estudios Tecnológicos de la Agencia Española de Protección de Datos ha emitido unas series de recomendaciones para tener en cuenta en caso de proteger nuestros datos personales en situaciones de movilidad y teletrabajo.

La empresa, como responsable del tratamiento, deberá tomar la decisión de que determinadas actividades de su empresa se ejecuten en situaciones de movilidad y teletrabajo. Dicha decisión puede formar parte de la estrategia de gestión, general o parcial para determinadas áreas o actividades (por ejemplo, personal que viaja con frecuencia) o puede ser motivada por situaciones excepcionales e incluso de fuerza mayor (por ejemplo, **el estado de alarma debido a la pandemia COVID-19**).

RECOMENDACIONES DIRIGIDAS A RESPONSABLES DEL TRATAMIENTO:

1. Definir una política de protección de la información para situaciones de movilidad: En dicha política hay que determinar qué formas de acceso remoto se permiten, qué tipo de dispositivos son válidos para cada forma de acceso y el nivel de acceso permitido en función de los perfiles de movilidad definidos. Así y como también, el personal tiene que estar informado sobre las principales amenazas por las que pueden verse afectados al trabajar desde fuera de la organización y las posibles consecuencias que pueden materializarse si se quebrantan dichas directrices, tanto para los sujetos de los datos como para la persona trabajadora.

2. Elegir soluciones y prestadores de servicio confiables y con garantías: Si se utilizan aplicaciones para realizar teletrabajo, éstas deberían tener las garantías suficientes y poder ofrecer soluciones con el fin de que eviten la exposición de los datos personales del personal, interesados y servicios corporativos de la organización.

3. Restringir el acceso a la información: Los perfiles o niveles de acceso a los recursos y a la información tienen que configurarse en función de los roles de cada persona empleada, de una forma incluso más restrictiva respecto de los concedidos en los accesos desde la red interna.

4. Configurar periódicamente los equipos y dispositivos utilizados en las situaciones de movilidad: Todos los equipos informáticos y los servidores tienen que estar actualizados y configurados para garantizar el desarrollo del teletrabajo por parte del personal. Se puede permitir el uso de dispositivos personales del personal siempre y cuando cumpla con la política de privacidad de la empresa y preste garantías en materia de seguridad y de protección de datos.

5. Monitorizar los accesos realizados a la red corporativa desde el exterior: Hay que establecer sistemas de monitorización encaminados a identificar patrones anormales en el trafico de red, como por ejemplo posibles ataques informáticos y brechas de seguridad. En esos casos, se debería notificar ante la Autoridad de Control (Agencia Española de Protección de Datos) en un plazo no superior a 72 horas. Estas monitorizaciones des de un acceso remoto deben respetar en todo momento los derechos digitales establecidos en la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales.

6. Gestionar racionalmente la protección de datos y la seguridad: Las medidas y garantías establecidas en las políticas definidas tienen que establecerse a partir de un análisis de riesgos en el que se evalúe la proporcionalidad entre los beneficios a obtener de un acceso a distancia y el impacto potencial de ver comprometido el acceso a la información de carácter personal.
También, se tiene que auditar los dispositivos con acceso remoto los procedimientos de administración y monitorización de la infraestructura, los servicios proporcionados por encargados y la forma en que la política es revisada y actualizada a los riesgos existentes.

RECOMENDACIONES DIRIGIDAS AL PERSONAL QUE PARTICIPA EN LAS OPERACIONES DE TRATAMIENTO:

1. Respetar la política de protección de la información en situaciones de movilidad definida por el responsable: Han de observarse las medidas y recomendaciones recogidas en las guías y política de protección de datos y seguridad de la información en situaciones de movilidad definidas por la organización, así como del resto de las normas y procedimientos que la desarrollen y, especialmente, lo que concierne al deber de confidencialidad de la persona trabajadora con relación a los datos personales a los que tuviera acceso en el desempeño de sus funciones laborales.

2. Proteger el dispositivo utilizado en movilidad y el acceso al mismo: La persona empleada deberá establecer un sistema de contraseñas lo suficientemente compleja para evitar el acceso ilícito a su dispositivo. No se debe descargar ni instalar aplicaciones o software que no hayan sido previamente autorizados por la organización. Una vez concluida la jornada de trabajo en situación de movilidad debe desconectarse la sesión de acceso remoto y apagar o bloquear el acceso al dispositivo.

3. Garantizar la protección de la información que se está manejando: En estos casos se tiene que extremar la confidencialidad de la información con la que el personal esta trabajando, si se trabaja con documentación en papel, se tiene que guardar en un lugar cerrado con llave para evitar el acceso ilícito y si se trabaja en formato digital establecer un sistema de contraseñas con el fin de proteger los datos de carácter personal.

4. Guardar la información en los espacios de red habilitados: Conviene evitar almacenar la información generada durante la situación de movilidad de forma local en el dispositivo utilizado, siendo preferible hacer uso de los recursos de almacenamiento compartidos o en la nube proporcionados por la organización. Si se permite la utilización de equipos personales, no utilizar bajo ningún concepto aplicaciones no autorizadas en la política de la entidad para compartir información.

5. Si hay sospecha de que la información ha podido verse comprometida comunicar con carácter inmediato la brecha de seguridad: Cualquier anomalía que pueda afectar a la seguridad de la información y a los datos personales tratados debe notificarse al responsable, sin dilación y a la mayor brevedad posible, a través de los canales definidos al efecto. Ante cualquier cuestión que puedan representar un riesgo para la protección de la información y el acceso a los recursos corporativos el empleado debe consultar con el Delegado de Protección de Datos y con el responsable de seguridad de la información, o los perfiles responsables designados al efecto, trasladándoles toda información de interés de la que tenga constancia.