Recomendaciones para proteger los datos personales en situaciones de movilidad y teletrabajo

La organización, como responsable del tratamiento, puede 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.

Si en el primer caso hay que realizar una planificación previa, en el segundo las circunstancias de urgencia pueden obligar a poner en marcha soluciones con carácter provisional. Cuando esto último sucede, es obligatorio, en paralelo y sobre todo cuando la situación se prolonga, realizar una reflexión y una adecuación de la implementación del teletrabajo. Hay que tener en cuenta que de ello depende la resiliencia del Estado, la continuidad de los procesos de negocio, y los derechos y libertades de los interesados cuyos datos se están tratando.

La organización y el personal que participa en las acciones de teletrabajo han de tener en cuenta las siguientes recomendaciones.

RECOMENDACIONES DIRIGIDAS A RESPONSABLES DEL TRATAMIENTO

A continuación, se enumeran un conjunto de recomendaciones para el responsable del tratamiento que éste tendrá que adecuar a la situación concreta de su objeto de negocio:

1. Definir una política de protección de la información para situaciones de movilidad

- Basada en la política de protección de datos y seguridad de la información de la entidad, y formando parte de ella, es necesario definir una **política específica para situaciones de movilidad** que contemple las necesidades concretas y los riesgos particulares introducidos por el acceso a los recursos corporativos desde espacios que no están bajo el control de la organización.
- 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. También deben definirse las responsabilidades y obligaciones que asumen las personas empleadas.
- Es necesario proporcionar guías funcionales adaptadas a formar a las personas empleadas, derivadas de dichas políticas, y que recojan al menos la información que se expone en el apartado “Recomendaciones dirigidas al personal que participa en las operaciones de tratamiento” de este mismo documento.
- El personal también ha de estar informado de 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.

- En dichas guías se debe identificar un punto de contacto para comunicar cualquier incidente que afecte a datos de carácter personal, así como los canales y formatos adecuados para realizar dicha comunicación.
- El personal ha de firmar un acuerdo de teletrabajo que incluya los compromisos adquiridos al desempeñar sus tareas en situación de movilidad.

2. Elegir soluciones y prestadores de servicio confiables y con garantías[1]

- Hay que evitar utilizar aplicaciones y soluciones de teletrabajo que no ofrezcan garantías y que puedan dar lugar a la exposición de los datos personales del personal, interesados y servicios corporativos de la organización, en particular, a través de los servicios de correo y mensajería.
- Hay que recurrir a proveedores y encargados que ofrezcan soluciones probadas y garantías suficientes que, en el mismo sentido, eviten la exposición de los datos personales del personal, interesados y servicios corporativos de la organización
- Si estos acceden a datos de carácter personal, tendrán la consideración de encargados de tratamiento y la relación se regirá por un contrato u otro acto jurídico que vincule al encargado respecto del responsable. Este contrato debe establecer el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable, de acuerdo con los términos establecidos en el artículo 28.3 del RGPD.

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.
- A su vez, hay que aplicar restricciones de acceso adicionales en función del tipo de dispositivo desde el que se acceda a la información (equipos portátiles corporativos securizados, equipos personales externos y dispositivos móviles como smartphones o tablets) y también dependiendo de la ubicación desde la que se accede.

4. Configurar periódicamente los equipos y dispositivos utilizados en las situaciones de movilidad

- Los servidores de acceso remoto han de ser revisados y hay que asegurar que están correctamente actualizados y configurados para garantizar el cumplimiento de la política de protección de la información para situaciones de movilidad establecida por la organización, así como el control de los perfiles de acceso definidos.
- Los equipos corporativos utilizados como clientes tienen que:
  - estar actualizados a nivel de aplicación y sistema operativo,
  - tener deshabilitados los servicios que no sean necesarios,

[1] El informe RBP/18 Recomendaciones de seguridad de situaciones de teletrabajo y refuerzo en vigilancia publicado por el CCN-CERT incluye controles y medidas de seguridad específicas a tener en cuenta durante una situación de trabajo en remoto, así como una relación de empresas que operan en nuestro país en el sector de la ciberseguridad y que ofrecen servicios y soluciones en el contexto de accesos remotos a los recursos corporativos.

  - tener una configuración por defecto de mínimos privilegios fijada por los servicios TIC que no pueda ser desactivada ni modificada por el empleado
  - instalar únicamente las aplicaciones autorizadas por la organización,
  - contar con software antivirus actualizado,
  - disponer de un cortafuegos local activado,
  - tener activados solo las comunicaciones (wifi, bluetooth, NFC, …) y puertos (USB u otros) necesarios para llevar a cabo las tareas encomendadas.
  - incorporar mecanismos de cifrado de la información.

- Si se permite el uso de dispositivos personales de las personas empleadas, al suponer un mayor riesgo por no incorporar los mismos controles de los equipos corporativos, además de exigir unos requisitos mínimos para poder utilizarlos en el establecimiento de conexiones remotas (por ejemplo, contar con un sistema operativo y software original y actualizado), hay que valorar la posibilidad de restringir la conexión a una red segregada que únicamente proporcione un acceso limitado a aquellos recursos que se hayan identificado como menos críticos y sometidos a menor nivel de riesgo.

5. Monitorizar los accesos realizados a la red corporativa desde el exterior

- Hay que establecer sistemas de monitorización encaminados a identificar patrones anormales de comportamiento en el tráfico de red cursado en el marco de la solución de acceso remoto y movilidad con el objetivo de evitar la propagación de malware por la red corporativa y el acceso y uso no autorizado de recursos.
- Las brechas de seguridad que afecten a datos personales han de comunicarse a la Autoridad de Control y/o a los interesados, con el propósito de crear un entorno de teletrabajo resiliente.
- Se debe informar al personal, en la política de protección de la información para situaciones de movilidad, sobre la existencia y el alcance de estas actividades de control y supervisión.
- Si las actividades de monitorización se usaran además para verificar el cumplimiento de las obligaciones laborales del personal, el responsable del tratamiento deberá informar con carácter previo, y de forma clara, expresa y concisa a las personas empleadas y, en su caso a sus representantes, de la medida adoptada en el marco de las funciones de control previstas en el Estatuto de los Trabajadores que han de ejercerse dentro de su marco legal y con los límites inherentes al mismo.
- Los mecanismos de monitorización implementados en el contexto de acceso remoto a recursos corporativos en situaciones de movilidad y teletrabajo deben respetar los derechos digitales establecidos en la LOPDGDD, en particular, el derecho a la intimidad y uso de dispositivos digitales y el derecho a la desconexión digital[2] en el ámbito laboral.
- La configuración definida para acceder a los recursos de forma remota debe ser revisada de forma periódica para garantizar que no ha sido alterada ni desactivada sin autorización además de permanecer actualizada y adaptada a un entorno externo de riesgo que evoluciona de manera continua.

[2] Artículos 87 y 88, respectivamente, de la LOPDGDD, https://www.boe.es/boe/dias/2018/12/06/pdfs/BOE-A-2018-16673.pdf

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.
   - En la política deben contemplarse los procedimientos internos para provisionar y auditar los dispositivos clientes de 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.
   - Los recursos que pueden ser accedidos se han de limitar en función de la valoración del riesgo que represente una pérdida del dispositivo cliente y la exposición o acceso no autorizado a la información manejada.
   - Hay que planificar y evaluar la aplicaciones y soluciones de acceso remoto teniendo en cuenta los principios de privacidad desde el diseño y por defecto a lo largo de todas las etapas de despliegue de la solución: desde la definición de los requisitos y necesidades hasta la retirada de la misma o de alguno de sus componentes[3].

RECOMENDACIONES DIRIGIDAS AL PERSONAL QUE PARTICIPA EN LAS OPERACIONES DE TRATAMIENTO

Las recomendaciones al personal han de estar recogidas en la política de teletrabajo del responsable, referenciadas en el acuerdo de teletrabajo y ajustadas a la situación concreta de las tareas a realizar. Una guía sobre el contenido de dichas recomendaciones es la siguiente:

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 debe definir y utilizar contraseñas de acceso robustas y diferentes a las utilizadas para acceder a cuentas de correo personales, redes sociales y otro tipo de aplicaciones utilizadas en el ámbito de su vida personal.
   - No se debe descargar ni instalar aplicaciones o software que no hayan sido previamente autorizados por la organización.

[3] El documento Guide to Enterprise Telework, Remote Access and Bring Your Own Device (BYOD) Security publicado por el NIST incluye una aproximación basada en el ciclo de vida que contempla recomendaciones y buenas prácticas a tener en cuenta en las fases de inicio, desarrollo, implementación, operación y mantenimiento y retirada de una solución de acceso remoto y teletrabajo.

- Es recomendable evitar la conexión de los dispositivos a la red corporativa desde lugares públicos, así como la conexión a redes WIFI abiertas no seguras.
- Deben mantenerse protegidos los mecanismos de autenticación definidos (certificados, contraseñas, tokens, sistemas de doble factor, …) para validarse ante los sistemas de control de acceso remoto de la organización.
- Si se dispone de un equipo corporativo, no se debe utilizar con fines particulares evitando el acceso a redes sociales, correo electrónico personal, páginas web con reclamos y publicidad impactante, así como otros sitios susceptibles de contener virus o favorecer la ejecución de código dañino.
- Si el equipo utilizado para establecer la conexión remota es personal, debe evitarse simultanear la actividad personal con la profesional y definir perfiles independientes para desarrollar cada tipo de tarea.
- El sistema antivirus instalado en el equipo debe estar operativo y actualizado.
- Siempre ha de verificarse la legitimidad de los correos electrónicos recibidos, comprobando que el dominio electrónico del que procede es válido y conocido, y desconfiando de la descarga de ficheros adjuntos con extensiones inusuales o el establecimiento de conexiones a través de enlaces incluidos en el cuerpo del correo que presenten cualquier patrón fuera de lo normal.
- Si pueden ser gestionadas por la persona empleada, conviene desactivar las conexiones WIFI, bluetooth y similares que no estén siendo utilizadas.
- 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

- Tanto en lugares públicos como en el entorno domésticos es obligado adoptar las precauciones necesarias para garantizar la confidencialidad de la información que se está gestionando.
- Si habitualmente se genera y trabaja con papel, durante situaciones de movilidad es importante minimizar o evitar la entrada y salida de documentación en este soporte y extremar las precauciones para evitar accesos no autorizados por parte de terceros.
- La información en soporte papel, incluyendo borradores, no se puede desechar sin garantizar que es adecuadamente destruida. Si es posible, no arrojar papeles enteros o en trozos en papeleras de hoteles, lugares públicos o en la basura doméstica a los que alguien podría acceder y recuperar información de carácter personal.
- Conviene extremar las precauciones para evitar el acceso no autorizado a la información personal, propia y de terceros, manejada, no dejando a la vista ningún soporte de información en el lugar donde se desarrolle el teletrabajo y bloqueando las sesiones de los dispositivos cuando estos estén desatendidos.
- Se debe evitar exponer la pantalla a la mirada de terceros. Si se trabaja habitualmente desde lugares públicos, es recomendable utilizar un filtro de privacidad para la pantalla.
- En la medida de lo posible es aconsejable prevenir que se puedan escuchar conversaciones por parte de terceros ajenos utilizando, por ejemplo,

auriculares o retirándose a un espacio en el que la persona empleada no esté acompañada.

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 (servicios en nube de alojamiento de archivos, correos personales, mensajería rápida, etc.)
- No se debe bloquear o deshabilitar la política de copia de seguridad corporativa definida para cada dispositivo.
- Es recomendable revisar y eliminar periódicamente la información residual que pueda quedar almacenadas en el dispositivo, como archivos temporales del navegador o descargas de documentos.

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 pueda suscitarse en el contexto de las situaciones de movilidad y 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.