

DIPUTACIÓ DE  
VALÈNCIA

*Protecció de Dades i Seguretat de la Informació*



# Boletín de protección de datos

Boletín del Departamento de protección de datos y Seguridad  
de la Información de la Diputación Provincial de Valencia

Boletín nº 1 | Julio 2020

**TELETRABAJO Y DESCONEXIÓN DIGITAL**



## PRESENTACIÓN



**Eusebio Moya**

*Responsable del Departamento de Protección  
de Datos y Seguridad de la Información.*

*Delegado de Protección de Datos de la  
Diputación Provincial de Valencia*

Hace aproximadamente veinte años la Diputación de Valencia creó la Unidad Técnica de Protección de Datos con el objetivo de garantizar el cumplimiento de la normativa legal e interna en materia de protección de datos, convirtiéndose de este modo en la primera administración pública en incorporar una unidad administrativa de estas características.

Desde aquel momento en que partimos de cero siempre hemos intentado compartir nuestra experiencia, puntos de vista e interpretaciones; no por ningún afán de protagonismo sino por poner a disposición de otras administraciones públicas, especialmente del ámbito local, elementos que pudieran ser útiles en una materia compleja y con tan poco arraigo en el sector público.

Hace tiempo que deseábamos elaborar alguna publicación que sumara también recursos en este ámbito. Y este deseo toma forma hoy a través de este Boletín, con el que pretendemos hacer nuestra modesta contribución al mundo de la protección de datos en el ámbito del sector público, especialmente en aquello que afecta a las Entidades Locales.

El Boletín de Protección de Datos Personales está dirigido a los empleados públicos en general, sin ser necesaria una formación específica en materia de protección de datos para una correcta asimilación de sus contenidos. En cada número se abordará un tema central al que se añadirán noticias de actualidad y otras referencias de interés. Comenzamos con un formato básico al que esperamos ir incorporando más secciones en un futuro.

El equipo del Departamento de Protección de Datos y Seguridad de la Información de la Diputación de Valencia esperamos que esta publicación os resulte interesante y que ayude a la difusión y mejor aplicación de la normativa de protección de datos personales.



Os invitamos a trasladarnos aquellas temáticas que resulten de vuestro interés para los próximos boletines informativos. Estas peticiones deberán dirigirse a:

Diputación de Valencia

Dpto. de Protección de Datos y  
Seguridad de la Información

Pl. de Manises, 4 46003 Valencia

email: [dpdssi@dival.es](mailto:dpdssi@dival.es)

## SUSCRIPCIONES

Si deseas suscribirse a nuestro Boletín informativo accede al siguiente

[enlace](#)



## ¿CÓMO Y QUÉ IMPLICA EL TELETRABAJO? DESCONEXIÓN DIGITAL

La crisis de la Covid-19, ha influido necesariamente en la forma de realizar nuestro trabajo; primero por el confinamiento impuesto por el estado de alarma y después por el aún elevado riesgo de contagios. Atendiendo a las recomendaciones realizadas por el Gobierno y a las circunstancias sobrevenidas para el desempeño del trabajo, ha resultado necesario, siempre que fuera posible, desarrollar la actividad profesional en modalidad de teletrabajo, conllevando ciertos riesgos y beneficios para la entidad y las personas trabajadoras.

Por ello, un gran número de empresas y entidades se ha sumado a esta iniciativa en España para mantener su actividad, ocasionando que el mercado laboral en España pasa por impulsar definitivamente la instauración del teletrabajo.

En este sentido, nos encontramos con una serie de disposiciones recogidas en las siguientes normas:

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD).
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica.
- Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores.
- O, Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.





El Artículo 13 del Estatuto de los Trabajadores regula la figura del teletrabajo como trabajo a distancia, en los siguientes términos:

***“Tendrá la consideración de trabajo a distancia aquel en que la prestación de la actividad laboral se realice de manera preponderante en el domicilio del trabajador o en el lugar libremente elegido por este, de modo alternativo a su desarrollo presencial en el centro de trabajo de la empresa.”.***

Asimismo, actualmente nos encontramos ante una revolución tecnológica que está cambiando la forma de entender nuestra forma de trabajar, viajar o relacionarnos y que, aunque no seamos conscientes de ello, requiere una preparación para:

- Un uso responsable de la tecnología en nuestro beneficio
- Evitar conductas de riesgo para la salud

## ¿QUÉ RIESGOS DEBEMOS TENER EN CUENTA?

Para la propia entidad, las conexiones remotas pueden ser una vía de entrada de código dañino a los sistemas, por ello, se considera clave poder garantizar la seguridad de estas conexiones y accesos. Así, debemos contar que los empleados conozcan una serie de buenas prácticas en el desempeño de sus funciones:

## DECÁLOGO BUENAS PRÁCTICAS EN TELETRABAJO

 <b>Uso personal y profesional:</b> Los dispositivos sólo pueden utilizarse para fines profesionales.	 <b>Necesidad de autorización:</b> cualquier extracción (información, equipamiento, etc.) de la organización requiere autorización.
 <b>Copias de seguridad:</b> sigue las instrucciones del departamento de informática.	 <b>Uso de canales de comunicación establecidos:</b> utiliza sólo los canales establecidos y autorizados.
 <b>Bloqueo de sesión:</b> bloquea el equipo cuando te ausentes de tu puesto de trabajo.	 <b>Evitar accesos no autorizados:</b> evita que personas no autorizadas vean o escuchen información.
 <b>Entorno de trabajo seguro:</b> no trabajes en estaciones, bares o similar.	 <b>Mantenimiento de los equipos:</b> cuida de tu equipo y manténlo actualizado
 <b>Normativa interna:</b> sigue la normativa de seguridad existente.	 <b>Gestión de incidencias:</b> comunica incidencias según el procedimiento habitual.



Con la finalidad de evitar y/o mitigar estos riesgos se debe trabajar en la promulgación de políticas internas que supongan una cultura preventiva o una guía de buenas prácticas relativas al uso adecuado de las TIC, y en tareas de sensibilización dirigidas al personal.

Además, se deben regular las pautas que permiten a los empleados desarrollar sus tareas desde ubicaciones externas a su centro de trabajo, garantizando la seguridad de los sistemas de información. Así, por ejemplo, en el caso de la Diputación de Valencia vienen recogidas en las “Normas de Seguridad de los Usuarios de los Sistemas de Información”, donde se describen cómo llevar a cabo el acceso remoto, la seguridad de los soportes electrónicos de información y las normas específicas de utilización de dispositivos portátiles y móviles.

Por otro lado, debemos conocer los riesgos existentes como empleados, dado que el desarrollo del teletrabajo puede afectar al equilibrio entre la vida profesional y personal y la salud, desdibujando la separación entre la jornada laboral y el tiempo de descanso.

Así, encontramos el derecho a la desconexión digital en el ámbito laboral, regulado en el artículo 88 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales:

***“Los trabajadores y los empleados públicos tendrán derecho a la desconexión digital a fin de garantizar, fuera del tiempo de trabajo legal o convencionalmente establecido, el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar”.***

***“El empleador, previa audiencia de los representantes de los trabajadores, elaborará una política interna dirigida a trabajadores, incluidos los que ocupen puestos directivos, en la que definirán las modalidades de ejercicio del derecho a la desconexión y las acciones de formación y de sensibilización del personal sobre un uso razonable de las herramientas tecnológicas que evite el riesgo de fatiga informática. En particular, se preservará el derecho a la desconexión digital en los supuestos de realización total o parcial del trabajo a distancia, así como en el domicilio del empleado vinculado al uso con fines laborales de herramientas tecnológicas”.***



En este sentido, el derecho a la desconexión digital es entendido, de un lado, como la obligación de conexión de las personas trabajadoras durante su jornada laboral, y de otro, como el derecho a la desconexión durante su tiempo de descanso sin que pueda verse interrumpido por el empleador. A saber, este derecho garantiza, fuera del tiempo de trabajo legal o convencionalmente establecido, el respeto del tiempo de descanso de las personas trabajadoras, permisos y vacaciones, así como de su intimidad personal y familiar. Este derecho de “nueva generación” tiene gran significado si lo trasladamos a la realidad actual del teletrabajo, dado que ante esta modalidad es mucho más sencillo que se desdibuje fácilmente la separación entre la vida profesional y personal de las personas trabajadoras.

Asimismo, el artículo 14.j.bis) del Estatuto Básico del Empleado Público reconoce a todos los empleados públicos el derecho:

***“A la intimidad en el uso de dispositivos digitales puestos a su disposición y frente al uso de dispositivos de videovigilancia y geolocalización, así como a la desconexión digital en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales”.***





En esta línea también se ha manifestado la propia Agencia Española de Protección de Datos (AEPD) estableciendo en sus Recomendaciones para proteger los datos personales en situaciones de movilidad y teletrabajo que *“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 desconexión digital en el ámbito laboral”*.

Además, así lo ha entendido el Ministerio de Trabajo y Economía Social, elaborando el anteproyecto de Ley de Trabajo a Distancia que tiene como marco el acuerdo europeo sobre teletrabajo, y cuyo texto se encuentra actualmente pendiente de negociación con los agentes sociales. Durante la crisis sanitaria no solo se ha reforzado la tendencia a la normalización del trabajo a distancia, sino que incluso su utilización se ha llegado a configurar como preferente, tanto en España como en otros países de nuestro entorno.

Teniendo en cuenta esto, **¿cómo debemos tratar el teletrabajo para reducir sus posibles riesgos?** Existe una doble vertiente protectora:

- De una parte, una protección reforzada frente a muchas veces inevitable invasión del tiempo de descanso del trabajador gracias a las herramientas de comunicación digital de las que dispone en su trabajo.
- Y de otra parte, se protege de los riesgos tecnológicos para la salud,

La implementación y efectividad del derecho a la desconexión digital descansa tanto en la persona trabajadora, que puede ejercerlo, como en el empleador, que ha de velar porque sea efectivo.

**En conclusión, existen dos vertientes a tener en cuenta para regular adecuadamente el derecho a la desconexión digital de los empleados, y que se protejan de los riesgos tecnológicos para su salud. De un lado, se debe contar con Políticas de Desconexión Digital que resulten efectivas y acordes a la realidad del tipo de trabajo desarrollado. Y, de otro, es necesario que se lleven a cabo tareas de sensibilización para que se conozcan los derechos sobre esta materia, y, sobre todo, como ejercerlos. Ambos aspectos son totalmente complementarios, dado que de nada serviría una regulación protocolizada de la desconexión digital sin los empleados conozcan cómo abordarlo y viceversa.**



## MATERIAL COMPLEMENTARIO

- Recomendaciones de la AEPD para proteger los datos personales en situaciones de movilidad y teletrabajo. Destacamos;
  1. "Respetar la política de protección de la información en situaciones de movilidad definida por el responsable
  2. Proteger el dispositivo utilizado en movilidad y el acceso al mismo
  3. Garantizar la protección de la información que se está manejando
  4. Guardar la información en los espacios de red habilitados
  5. Si hay sospecha de que la información ha podido verse comprometida comunicar con carácter inmediato la brecha de seguridad"
- Consejos para proteger los datos personales cuando teletrabajamos del Consejo de Transparencia y Protección de datos de Andalucía. Destacamos algunas de ellas;
  1. "Si el equipo que utilizas te lo ha facilitado tu organismo, no lo emplees además para un uso particular. Si el equipo es de tu propiedad, no simultanees las tareas laborales con las particulares: cada cosa en su momento. Para facilitar esto, si se trabaja con equipos propios, es aconsejable crear un perfil profesional en el equipo con el adecuado control de acceso.
  2. Tanto si el teletrabajo se realiza desde un equipo del organismo o desde uno particular, asegúrate de que dispone de un antivirus que está operativo y se actualiza adecuadamente.
  3. No almacenes en el disco duro local del equipo con el que teletrabajas información que incluya datos personales; utiliza para ello el almacenamiento en red que te proporciona tu organismo. [...]"
- Buenas prácticas y recomendaciones de seguridad del Instituto Nacional de Ciberseguridad (INCIBE)

## NOTICIAS

- Se da luz verde para probar en la isla canaria de La Gomera una app de Teléfono móvil que permitirá notificar a los contactos de un usuario el posible riesgo de contagio por #COVID19. [Consulta en este enlace](#).
- Desde las Agencia Española de Protección de Datos se analiza cómo afecta a nuestra Privacidad esta y otras medidas en tiempos de pandemia. [Consulta este enlace](#) con las indicaciones.
- ¿Tomar la temperatura en la entrada de espacios públicos y privados? Desde la Agencia Española de Protección de Datos lanzan un comunicado en relación con la toma de temperatura por parte de comercios, centros de trabajo y otros establecimientos. [Consulta este enlace](#) con las implicaciones.
- El Tribunal Supremo confirma una multa de 40.000 euros de Protección de Datos a Mutua Madrileña por la publicidad que recibió un cliente que rechazó expresamente el uso de sus datos ejerciendo su derecho de oposición a publicidad. [Consulta este enlace](#) con la noticia.
- Durante estos días de confinamiento los menores pasan más tiempo del habitual conectados a internet, por lo que la Agencia Española de Protección de Datos ofrece consejos y recomendaciones a madres y padres para que puedan protegerles de los contenidos inadecuados. [Consulta este enlace](#) con las recomendaciones.
- La Agencia Española de Protección de Datos (AEPD) ha suscrito la 'Declaración de teletrabajo e innovación: 12 compromisos + 12 causas' de Women in a Legal World, convirtiéndose en el primer organismo de la Administración General del Estado que se adhiere a la iniciativa. El apoyo a esta Declaración se engloba en el marco de la Responsabilidad Social y Sostenibilidad de la Agencia y su Plan de Igualdad, que incluye una apuesta firme por esta modalidad laboral también en el ámbito de las Administraciones Públicas. [Consulta este enlace](#).