PROTOCOLO Y POLÍTICAS INTERNAS DE DESCONEXIÓN DIGITAL
ALUSIN SOLAR, S.L.U

MANUAL PARA LAS PERSONAS TRABAJADORAS

25/04/2025

INTRODUCCIÓN Y FUNDAMENTOS DE DERECHO

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPD) introduce el derecho de las personas trabajadoras a la desconexión digital en el marco del derecho a la intimidad en el uso de dispositivos digitales en el ámbito laboral.

En concreto, el artículo 88 establece que las personas trabajadoras *'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.'*

En este sentido, el citado artículo destaca la necesidad de adaptar las modalidades de ejercicio de este derecho a la naturaleza y objeto de la relación laboral a fin de que se potencie el derecho a la conciliación de la actividad laboral y la vida personal y familiar, atendiendo especialmente a las situaciones particulares de trabajo a distancia, ya sea total o parcial, y/o al supuesto relativo a la utilización de dispositivos móviles personales para el uso profesional.

Se define, asimismo, la obligación de las empresas de elaborar, previa audiencia de los representantes de las personas trabajadoras, una política interna dirigida a personas trabajadoras, incluyendo directivos, definiendo las modalidades de ejercicio del derecho, así como aquellas acciones de formación y sensibilización diseñadas de cara a evitar la fatiga informática, tecnoestrés o burnout.

Cabe señalar que la Disposición Adicional Decimotercera de la LOPD introduce asimismo la modificación del Texto Refundido de la Ley del Estatuto de los Trabajadores, introduciendo el artículo 20 bis, que establece que las personas trabajadoras *"tienen derecho a la intimidad en el uso de los dispositivos digitales puestos a su disposición por el empleador, a la desconexión digital y a la intimidad frente al uso de dispositivos de videovigilancia y geolocalización en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales*'.

Por todo ello, en cumplimiento con lo establecido en la normativa referenciada y con el fin de dar respuesta a la necesidad de establecer una delimitación inequívoca entre la jornada laboral y el tiempo de descanso de las personas trabajadoras -en el que se incluyen los descansos, vacaciones, días de asuntos propios, libranzas, descanso diario y semanal, permisos, incapacidades y/o excedencias- y de cara a proveer a las mismas de cobertura y protección adecuada en lo relativo al ejercicio del derecho de desconexión digital, la ENTIDAD ALUSIN SOLAR, S.L.U (en adelante, ENTIDAD) a elaborar la presente POLÍTICA INTERNA o MANUAL DE DESCONEXIÓN DIGITAL, que pondrá a disposición de las personas trabajadoras, y que tiene por objeto potenciar tanto el reconocimiento como el ejercicio del derecho de desconexión digital, resultando de obligatorio cumplimiento por parte de la ENTIDAD, sin perjuicio de lo establecido en los acuerdos que mediante negociación colectiva se formalicen o se puedan formalizar en el futuro.

Asimismo, la ENTIDAD se rige por lo establecido en el convenio colectivo METAL

DEFINICIONES

AEPD Agencia Española de Protección de Datos

BYOD (Bring Your Own Device) Método de trabajo que supone la utilización de dispositivos móviles personales para uso profesional, generalmente mediante la incorporación de los mismos a las redes corporativas, generando por tanto un uso compartido tanto para tareas profesionales de uso corporativo como para las personales de los empleados.

Empleado persona que voluntariamente presta sus servicios retribuidos por cuenta ajena y dentro del ámbito de organización y dirección de otra persona, física o jurídica, denominada empleador o empresario.

ETReal Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores.

INCIBE Instituto Nacional de Ciberseguridad

LOPD Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

RGPD 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 o Reglamento europeo de Protección de Datos.

CANAL DE DENUNCIAS O WHISTLEBLOWING

La ENTIDAD establecerá un canal de denuncias interno que permita la comunicación de irregularidades de potencial trascendencia e incidencias en lo relativo a la protección del ejercicio del derecho de desconexión digital.

En caso de ya disponer de un canal de denuncias resultado de la elaboración previa de un Manual de Prevención de Delitos en materia de Compliance, dicha vía podrá utilizarse en materia de desconexión digital.

En este sentido, se configura la dirección de correo electrónico lorena.monteiro@alusinsolar.com a tal efecto. Asimismo, las personas trabajadoras podrán dirigirse a la dirección de correo electrónico indicada con el fin de trasladar sus consultas, sugerencias, dudas o cualquier cuestión relacionada con la materia de desconexión digital, pudiendo asimismo solicitar ayuda o soporte técnico de cara a implantar e interpretar las medidas de seguridad establecidas en estas políticas.

Además, la ENTIDAD ha establecido la siguiente vía para uso de los empleados como canal de desconexión digital: Formualrio Web.

FORMACIÓN E INFORMACIÓN

Para cumplir adecuadamente con lo establecido en la legislación vigente, la implantación de las medidas recogidas en esta Política debe ir acompañada de la difusión adecuada del mismo y de su explicación a los Empleados y, en su caso, directivos.

Se ha de enfatizar por tanto en la importancia de su cumplimiento y la asunción por parte de la ENTIDAD de los principios de actuación tendentes a promover el ejercicio correcto del derecho de desconexión digital de las personas trabajadoras.

Por ello, la ENTIDAD facilitará a los Empleados información periódica sobre las políticas de desconexión digital adoptadas por la misma.

En este sentido, los Manuales de Desconexión Digital, así como las políticas y procedimientos internos estarán disponibles para todos los Empleados y, en su caso, directivos.

Se organizarán, al menos una vez al año, sesiones de formación para personas trabajadoras, incluyendo en su caso a directivos, con las siguientes finalidades:

· Dar a conocer el derecho a la desconexión digital, así como sus modalidades de ejercicio, medidas, etc.

· Explicar en qué consisten las situaciones en las que el derecho a la desconexión digital de los empleados pueda verse vulnerado o amenazado.

· Recordar cuáles son las medidas técnicas adoptadas en cuanto al uso de dispositivos BYOD, en su caso.

El contenido de las citadas sesiones de formación tendrá en cuenta las funciones y responsabilidades de aquellos a los que estén dirigidas. La ENTIDAD será la encargada de promover y ejecutar la organización y contenido de las sesiones, pudiendo valerse, para ello, de empresas externas especializadas.

El objetivo último de las sesiones de formación es garantizar que los asistentes conocen sus derechos en materia de desconexión digital, así como las modalidades de ejercicio; evitar cualquier vulneración o amenaza a este derecho y representar un canal de comunicación entre las personas trabajadoras y la ENTIDAD, al objeto de detectar cualquier preocupación, duda o recomendación que pudieran tener en relación con la desconexión digital.

Actualmente, la ENTIDAD no está realizando actividades formativas en este sentido.

IDENTIFICACIÓN DE PUESTOS DE TRABAJO

Se ha procedido a realizar una identificación de los puestos de trabajo en la ENTIDAD y se ha llegado a la siguiente conclusión:

La ENTIDAD cuenta con personal contratado en situación de teletrabajo o trabajo a distancia.

Todos los empleados que se encuentran en situación de teletrabajo o trabajo a distancia utilizan dispositivos corporativos.

POLÍTICA CORPORATIVA EN MATERIA DE DESCONEXIÓN DIGITAL

En cumplimiento de la exigencia de la normativa reguladora del derecho a la desconexión digital, la ENTIDAD procede a la adopción de una serie de medidas que tienden a asegurar el respeto a este derecho, incluyendo el respeto del tiempo de descanso y vacaciones de las personas trabajadoras, así como de su intimidad familiar y personal independientemente de la jornada y horario ordinarios de trabajo.

Por lo tanto, las disposiciones que se exponen a continuación resultan de obligado cumplimiento para la entidad, encargada de velar por el respeto al derecho de desconexión digital:

- Las personas trabajadoras tienen derecho a no responder ninguna comunicación que reciban fuera de su jornada laboral o en periodos de descanso y vacaciones, independientemente del medio utilizado.

- Con carácter excepcional, este apartado no será de aplicación en caso de que concurran excepcionales de fuerza mayor o que supongan un grave, inminente o evidente perjuicio empresarial o del negocio, cuya urgencia temporal necesita indubitadamente de una respuesta inmediata. En estos casos, el tiempo de trabajo computará como hora extraordinaria.

- Las personas trabajadoras se comprometen al uso adecuado de los medios informáticos y tecnológicos puestos a disposición por la empresa, en su caso, evitando en la medida de lo posible su empleo fuera de la jornada estipulada.

- Los superiores jerárquicos y compañeros se abstendrán de requerir respuesta en las comunicaciones enviadas a las personas trabajadoras fuera de horario de trabajo o próximo a su finalización, siempre que pudieran suponer para los destinatarios de las mismas la realización de un trabajo efectivo que previsiblemente pueda prolongarse e invadir su tiempo de descanso. Se promueve asimismo el uso de la función de envío programado, de forma que la comunicación pueda entregarse a persona trabajadora al inicio de su siguiente jornada laboral.

- En caso de enviar una comunicación que pueda suponer respuesta fuera del horario establecido al efecto, el remitente (directivo o persona trabajadora de la entidad) asumirá expresamente que la respuesta se producirá en la jornada laboral siguiente

- Se respeta el derecho de desconexión digital de las personas trabajadoras durante sus vacaciones, días de asuntos propios, libranzas, descanso diario y semanal, permisos, incapacidades o excedencias, en los mismos términos.

- Al iniciar sus periodos vacacionales, las personas trabajadoras tendrán la obligación de configurar un mensaje de respuesta automático a los emails recibidos, derivar a una persona encargada, repartir las tareas,

- Asimismo, al terminar la jornada laboral, se procederá a apagar los dispositivos,

- Se restringe el uso de equipos y dispositivos ajenos que no estén autorizados por la empresa, para conectarse a las redes corporativas.

- Resulta necesaria la firma de un documento de conformidad y aceptación de la política corporativa de uso de dispositivos móviles personales y actuar conforme a las exigencias en la misma establecidas.

- Se promueve el respeto y adopción de las medidas de seguridad establecidas en esta política en lo relativo a los dispositivos personales de uso profesional (BYOD), en su caso.

- Prestar ayuda y soporte a las personas trabajadoras, en caso de que lo requieren, en lo relativo al cumplimiento de los requisitos técnicos de seguridad establecidos en esta política (configuración de parámetros de seguridad, descarga y actualización de antivirus, etc.)

- Mantener actualizadas y revisadas las políticas de seguridad corporativas.

- Se promueven actividades de información, sensibilización y formación de las personas trabajadoras y, en su caso, directivos o superiores jerárquicos en materia de desconexión digital.

- Queda prohibida la posibilidad de sancionar disciplinariamente a las personas trabajadoras con motivo del ejercicio de su derecho de desconexión digital, que no podrá repercutir negativamente en su desarrollo profesional.

GUÍA DE HERRAMIENTAS DIGITALES Y CONSIDERACIONES ESPECIALES EN EL USO DE DISPOSITIVOS PERSONALES (BYOD)

El teletrabajo o el trabajo a distancia ha promovido la generalización del método de trabajo BYOD (por sus iniciales en inglés, Bring Your Own Device), que se caracteriza por el hecho de que los empleados puedan hacer uso, desde cualquier lugar (incluyendo el domicilio particular y la propia oficina) de dispositivos móviles personales incorporados a las redes corporativas, de forma que se acepta su uso compartido, que incluye tanto tareas profesionales como las funcionalidades derivadas del uso personal cotidiano.

Todo ello puede entrañar una serie de riesgos de seguridad para las empresas, como pueden ser los derivados de las siguientes situaciones:

- Pérdida, robo o destrucción de dispositivos
- Robo de credenciales
- Pérdida de información
- Conexión a redes no seguras
- Geoposicionamiento

La Guía de dispositivos móviles personales para uso profesional (BYOD) establece una serie de consideraciones a tener en cuenta al hacer uso de estos dispositivos en las empresas y subraya la importancia de involucrar, concienciar y formar a los usuarios de dichos dispositivos para que estén capacitados para un uso responsable y correcto de los mismos.

Medidas técnicas de configuración

Los dispositivos BYOD deberán configurarse de forma que se refuerce la seguridad de los mismos, y por tanto, no quede comprometida la seguridad de la información empresarial que pueda almacenar.

En este sentido, la entidad establece una serie de requisitos de configuración de los dispositivos personales que se utilicen con fines profesionales.

En primer lugar, el dispositivo debe contar con la instalación, configuración y actualización de un sistema de antivirus.

Se deben configurar sistemas de autenticación robustos de dispositivos y aplicaciones mediante el uso de contraseñas, patrones, pines, etc. que sólo conozca el usuario del dispositivo BYOD, así como deshabilitar la funcionalidad de 'recordar contraseña o credenciales', de forma que haya que introducirla manual e individualmente cada vez que se vaya a acceder a una aplicación.

También es importante hacer uso de sistemas de cifrado de datos y comunicaciones, apartado que se desarrollará más adelante.

Asimismo, el dispositivo deberá estar configurado de forma que se realicen las actualizaciones de software pertinentes.

Instalación de aplicaciones

Se evitará, en la medida de lo posible, la instalación de aplicaciones de terceros en los dispositivos, así como de aquellas aplicaciones personales que puedan suponer un riesgo para la confidencialidad de la información empresarial almacenada.

En este sentido, queda prohibida la instalación de aplicaciones de fuentes no seguras y/o de no confianza, ya que pueden contener malware.

A la hora de descargar o instalar programas o aplicaciones, es imprescindible, asimismo, limitar la concesión de permisos de las mismas a lo estrictamente necesario para su correcto funcionamiento, prestando especial atención a este apartado y evitando la posibilidad de que se produzca una modificación en la configuración de los dispositivos que pueda dar lugar a la concesión de permisos adicionales de forma no autorizada o eliminar limitaciones propias del sistema de seguridad de los dispositivos.

Por todo ello, a la hora de descargar e instalar una aplicación o programa, habrá que tener en cuenta una serie de medidas, como son las siguientes:

- Comprobar que la aplicación o programa a descargar o instalar se encuentra entre los permitidos en las políticas de seguridad de la entidad.
- Leer atentamente los términos y condiciones de uso e instalación.
- Revisar los permisos, así como el alcance de los mismos.
- Realizar las descargas únicamente a través de los markets oficiales de Android e iOS (Play Store y App Store respectivamente).

En caso de duda, se recomienda encarecidamente a los trabajadores que planteen la cuestión a su superior o a la persona o departamento encargados de la gestión de la seguridad de los dispositivos y sistemas de la empresa. También será posible trasladar dudas o consideraciones a través del canal de denuncias de la entidad y/o a la dirección de email designada a tal efecto.

Realización y almacenamiento de copias de seguridad

Según la Guía de dispositivos móviles personales para uso profesional del INCIBE, la empresa debe hacer copias de seguridad de la información empresarial, lo que incluye también aquella almacenada en los dispositivos BYOD.

En este sentido, tanto la Agencia Española de Protección de Datos como el INCIBE indican que las copias de seguridad deben almacenarse fuera del propio dispositivo, ya sea en nube o en servidores corporativos.

Estos organismos recomiendan que dichas copias de seguridad se realicen de manera automática y periódica, permitiendo asimismo que puedan realizarse complementariamente de forma manual. También insisten en la importancia de que sea la empresa la que almacene, custodie y controle los dispositivos en los que se guarden las copias de seguridad, lo cual es preferible a la utilización de dispositivos personales a tal fin.

De esta forma, en el caso de que se utilicen dispositivos BYOD que almacenen información empresarial objeto de backup, la empresa debe velar por la protección de la privacidad de los datos personales de la persona trabajadora que el dispositivo pueda contener.

La normativa de protección de datos exige, como regla general, que las copias de seguridad se realicen con una periodicidad, al menos, semanal. Fuera de este requisito, es la propia empresa la que deberá determinar el sistema de almacenamiento, así como el número y la periodicidad de las copias de seguridad en función de sus propias necesidades, así como de variables como el tipo de dispositivos, el volumen y tipo de información, etc.

En el caso de que la entidad subcontrate el servicio de backup con una empresa externa, además de formalizar los correspondientes contratos de encargado de tratamiento de datos personales y tras confirmar la adaptación y cumplimiento de la normativa de protección de datos por parte del proveedor, este último deberá asimismo facilitar información sobre el tipo y frecuencia con la que realiza copias de seguridad de sus servidores, la disponibilidad de los datos objeto de copia de seguridad en cualquier momento y situación (incidentes de seguridad, mantenimiento, etc.), posibles restricciones, procedimientos de actuación en caso de fallo de servicio, tiempos de indisponibilidad, medidas de protección, etc...

Cifrado de la información

Se debe hacer uso del sistema de cifrado interno de datos y dispositivos mediante contraseñas de acceso, pines, patrones o nivel de arranque, de cara a evitar comprometer la seguridad de la información empresarial en caso de pérdida, robo o situaciones análogas,

De esta forma, la información queda protegida frente a accesos ilegítimos por parte de terceros o personas no autorizadas, utilizando un algoritmo de cifrado y/o una contraseña, en función de las posibilidades que ofrezca el propio dispositivo.

Esta obligación podría incluso extenderse al intercambio de correos electrónicos y comunicaciones.

Geoposicionamiento

La entidad desaconseja la habilitación de la función de geolocalización o ubicación del dispositivo en caso de que su uso no sea estrictamente necesario, así como la concesión de permisos en la instalación o utilización de aplicaciones y programas que puedan solicitar el acceso a la misma.

En caso de que la entidad requiera la habilitación de la herramienta de geoposicionamiento del dispositivo BYOD, informará previamente y recabará su consentimiento expreso de conformidad con lo establecido en la normativa de protección de datos.

Actualmente, la ENTIDAD no utiliza sistemas de geoposicionamiento de dispositivos de los empleados

Herramientas en remoto

Los dispositivos BYOD y ciertas herramientas comerciales ofrecen una serie de funcionalidades que pueden resultar útiles en caso de que su produzca la pérdida o robo de terminales que contengan información empresarial.

Con el fin de velar por la privacidad, así como por el derecho a la intimidad y el honor de las personas trabajadoras, la entidad sólo podrá hacer uso de estas funcionalidades en los casos en los que sea estrictamente necesario.

Mediante estas herramientas, se puede lograr la localización de terminales mediante GPS, WiFi o antena de telefonía:- Localización remota

Conexiones a redes externas (WiFi y VPN)

En relación a las conexiones WiFi, la entidad establece una serie de pautas a tener en cuenta por parte de los usuarios de dispositivos BYOD, tanto a la hora de realizar tareas profesionales como en el uso de los mismos a nivel personal.

En primer lugar, se desaconseja encarecidamente el uso de redes públicas desprotegidas, gratuitas o no seguras (por ejemplo, en hoteles, aeropuertos u hospitales) alentando el uso de redes 3G, 4G (o 5G) en su lugar, así como de redes privadas seguras y de confianza.

Asimismo, es importante que los usuarios de dispositivos BYOD desconecten la función de conexión WiFi en el caso de que no vayan a hacer uso de la misma, e impidan la conexión automática a redes disponibles.

En el caso de que no exista alternativa al uso de conexiones no seguras, debe hacerse uso de una red privada virtual o VPN (de sus siglas en inglés, Virtual Private Network), de forma que se creen 'canales seguros cifrados de comunicación que garanticen la confidencialidad' de la información del dispositivo y se confirme la comunicación segura entre dispositivos previamente autorizados.