



# **EL TELETRABAJO COMO NUEVO PARADIGMA PARA LA PRESTACIÓN DE SERVICIOS ENTRE TRABAJADORES Y EMPRESAS: PREGUNTAS Y RESPUESTAS**



**Grupo IT Digital de AUTELSI**

**Febrero 2022**

## Índice

INTRODUCCIÓN	2
EJE 1 – ASPECTOS LEGALES, PRIVACIDAD Y COMPLIANCE	3
EJE 2 - RIESGOS LABORALES Y PSICOSOCIALES Y ERGONOMÍA	7
EJE 3 - INFRAESTRUCTURA Y RIESGOS DE CIBERSEGURIDAD	9
EJE 4 - CULTURA: CONCIENCIACIÓN, FORMACIÓN Y CAPACITACIÓN	12
EJE 5 - PRODUCTIVIDAD Y NEGOCIO	15
ANEXO - ALGUNOS DATOS SOBRE TELETRABAJO	18
AUTORES	21

## Introducción

Desde el inicio de la pandemia convivimos con el teletrabajo, independientemente de las circunstancias personales de cada uno, y de si nos gusta o no este modelo.

Antes ya había muchas empresas que ofrecían este modelo como uno más; sin embargo, la pandemia ha obligado a empresas con un esquema presencial a modificar de la noche a la mañana su modelo e implementar el teletrabajo como única forma de prestación de servicios.

A partir de ahora, con el previsible fin de la pandemia, se plantea un nuevo paradigma tanto para las empresas como para los trabajadores: la implementación del teletrabajo como una nueva forma de prestar los servicios que muchos trabajadores demandan de forma más definitiva, hasta el punto de que algunos estarían dispuestos a cambiar de empresa si la actual no les permite teletrabajar.

Las empresas están dando respuesta a esta demanda facilitando cada vez más el teletrabajo, a veces de forma completa y otras con un sistema mixto teletrabajo / presencial. Contamos ya con la Ley 10/2021, de 9 de julio, que regula el trabajo a distancia y el Gobierno está trabajando en el Proyecto de Real Decreto por el que se regulará el Teletrabajo en la Administración General del Estado

Conscientes de los muchos retos, pero también de las muchas oportunidades que genera esta situación, en Autelsi hemos creado un grupo de trabajo para reflexionar sobre este tema y compartir experiencia con una perspectiva amplia, considerando los muchos aspectos que conlleva. El trabajo que te presentamos es el primer resultado de los debates de este grupo.

Se trata de un documento de preguntas y respuestas rápidas articuladas en cinco ejes, recogiendo la experiencia de los expertos y empresas participantes.

Los cinco ejes son:

- Aspectos Legales, Privacidad y Cumplimiento
- Riesgos Laborales y Psicosociales y Ergonomía
- Infraestructura y Riesgos de Ciberseguridad
- Cultura, Formación y Capacitación
- Productividad y Negocio

Además, se añade un análisis con datos sobre la situación actual del teletrabajo en España.

Con esta primera entrega el grupo ha querido dar una respuesta pronta, a un tema candente sobre el que las empresas se encuentran ahora mismo tomando decisiones. Continuamos trabajando en una segunda entrega en la que se ampliará el estudio en cada uno de los ejes mediante una consulta a empresas y organismos de la Administración Pública, incluyendo también no asociados.

Agradecemos a todos los miembros por su trabajo, aportaciones, y sobre todo por compartir las experiencias personales y de su empresa. Esperamos que este documento te sea útil, y si es así estaremos contentos de haber cumplido con nuestro objetivo.

## Eje 1 – Aspectos legales, privacidad y compliance

---

### *1.- ¿Es voluntario el teletrabajo tanto para la empresa como para el trabajador?*

---

La Ley de Trabajo a Distancia (Ley 10/2021 de 9 de julio) establece claramente que el trabajo a distancia (conocido como “teletrabajo” cuando es desarrollado por medios telemáticos) “será voluntario para la persona trabajadora y para la empleadora y requerirá la firma del acuerdo de trabajo a distancia regulado en esta Ley”.

Por ello, desde el punto de vista de las empresas, éstas no pueden imponer el teletrabajo a los trabajadores por la vía de la modificación sustancial de sus condiciones de trabajo, ni tampoco cabe que, su negativa a teletrabajar, les pueda suponer consecuencias disciplinarias.

Igualmente, desde el punto de vista de los trabajadores, éstos solo podrán alegar un derecho a trabajar a distancia que imponer frente a la voluntad del empresario cuando así lo prevea la Ley, el convenio colectivo de aplicación o los pactos de empresa suscritos con los representantes de los trabajadores.

Ejemplos de previsiones legales que excepcionan la norma general de voluntariedad serían el teletrabajo como medida de apoyo al cumplimiento de las obligaciones derivadas de la prevención de riesgos laborales (por ejemplo, priorizándolo cuando sea técnica y razonablemente posible, como freno de un brote de COVID en el centro de trabajo), el teletrabajo solicitado como medida conciliación de la vida familiar y laboral (la adaptación de la jornada prevista en el art. 34.8 del Estatuto de los Trabajadores) o el Plan MECUIDA prorrogado hasta el 28/2/2022. Todo ello, bajo determinadas circunstancias a ponderar en cada caso.

Por último, mencionar que, además de ser voluntaria, la decisión de trabajar a distancia también es reversible para ambas partes, de nuevo según lo establecido en la negociación colectiva o, en su defecto, en el acuerdo de trabajo a distancia.

### *2.- ¿Qué debe recoger el acuerdo de teletrabajo como mínimo y con quién se negocia?*

---

El acuerdo está regulado en la citada Ley 10/2021, de 9 de julio. Se entenderá que es “regular” (y por tanto que está bajo el ámbito de aplicación de esta Ley) el trabajo a distancia que se preste, en un periodo de referencia de tres meses, un mínimo del treinta por ciento de la jornada o el porcentaje proporcional equivalente en función de la duración del contrato de trabajo.

El teletrabajo pasará siempre por un acuerdo escrito entre la empresa y la persona empleada. Este acuerdo podrá formar parte del contrato inicial o realizarse en un momento posterior y ello con carácter previo al comienzo del trabajo a distancia. La empresa deberá remitir en 10 días una copia del acuerdo a la representación de los trabajadores, que posteriormente se enviará a la Oficina de Empleo. El acuerdo deberá contener como mínimo:

- a) Inventario de los medios, equipos y herramientas que exige el desarrollo del trabajo a distancia concertado, incluidos los consumibles y los elementos muebles, así como de la vida útil o periodo máximo para la renovación de estos.
- b) Enumeración de los gastos que pudiera tener la persona trabajadora por el hecho de prestar servicios a distancia, así como la forma de cuantificación de la compensación que obligatoriamente debe abonar la empresa y momento y forma para realizar la misma, que se corresponderá, de existir, con la previsión recogida en el convenio o acuerdo colectivo de aplicación.
- c) Horario de trabajo de la persona trabajadora y dentro de él, en su caso, reglas de disponibilidad.
- d) Porcentaje y distribución entre trabajo presencial y trabajo a distancia, en su caso.
- e) Centro de trabajo de la empresa al que queda adscrita la persona trabajadora a distancia y donde, en su caso, desarrollará la parte de la jornada de trabajo presencial.
- f) Lugar de trabajo a distancia elegido por la persona trabajadora para el desarrollo del trabajo a distancia.
- g) Duración de los plazos de preaviso para el ejercicio de las situaciones de reversibilidad, en su caso.
- h) Medios de control empresarial de la actividad.
- i) Procedimiento a seguir en el caso de producirse dificultades técnicas que impidan el normal desarrollo del trabajo a distancia.
- j) Instrucciones dictadas por la empresa, con la participación de la representación legal de las personas trabajadoras, en materia de protección de datos, específicamente aplicables en el trabajo a distancia.
- k) Instrucciones dictadas por la empresa, previa información a la representación legal de las personas trabajadoras, sobre seguridad de la información, específicamente aplicables en el trabajo a distancia.
- l) Duración del acuerdo de trabajo a distancia.

---

*3.- ¿Cómo se garantiza el cumplimiento de las obligaciones que en materia de protección de datos personales debe cumplir la empresa con relación a los datos personales objeto de tratamiento?*

---

El derecho a la protección de datos es un derecho de carácter fundamental, reconocido en el artículo 18.4 de la Constitución Española, que fue desarrollado a través de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos Personales y, posteriormente, por la actual Ley Orgánica 3/2018, de 5 de febrero de Protección de Datos Personales y Garantía de los Derechos Digitales, que aplica directamente las disposiciones establecidas en el Reglamento Europeo de Protección de Datos (UE 2016/679, de 26 de abril de 2016).

En el ámbito del teletrabajo, el Responsable del Tratamiento, debe establecer unas políticas y procedimientos para garantizar los derechos que en el ámbito de protección de datos se reconocen a los trabajadores y a las personas físicas que se relacionan con el Responsable del Tratamiento y cuyos datos son objeto de tratamiento.

Esto va a suponer la necesidad de definir primero una estrategia de planificación sobre en qué va a consistir el teletrabajo, el ámbito y cómo se va a desarrollar, para luego establecer las políticas y procedimientos necesarios para que los derechos de ambos titulares de datos

personales queden garantizados y los mismos sean tratados conforme a los principios establecidos en el artículo 5 del Reglamento General de Protección de Datos (RGPD).

Desde el punto de vista de los trabajadores que realicen el teletrabajo, en el caso que el tratamiento de sus datos y tipología de datos se vea ampliada, habrá que tener en cuenta cómo juega el principio de licitud del tratamiento y recurrir a bases legitimadoras para el tratamiento de los datos, diferentes al consentimiento, como la ejecución del propio contrato que regularice ese teletrabajo; el cumplimiento de obligaciones legales o el cumplimiento de un interés legítimo del empleador.

En el caso que, como consecuencia del teletrabajo, se traten datos especialmente protegidos por la normativa, como pueden ser los biométricos, necesarios para un control y monitorización del trabajo, la prohibición de ese tratamiento puede verse levantada en base a alguno de los supuestos previstos en el artículo 9.2 del RGPD, siempre y cuando se garanticen los derechos y libertades fundamentales y el control sea estrictamente necesario y dentro del ámbito exclusivamente laboral.

Por último, es importante tener en cuenta que, como en el caso del trabajo presencial, en el ámbito del teletrabajo también va a existir una expectativa de privacidad y deberá respetarse el derecho a la intimidad del trabajador, así como el derecho a la desconexión digital, por lo que deberá establecerse cómo se realiza la supervisión del trabajo y, en su caso, la monitorización.

Desde el punto de vista de los derechos de las personas físicas que se relacionan con el Responsable del Tratamiento, cuyos datos se tratan, se deberá analizar si los nuevos medios de trabajo garantizan el cumplimiento de los principios establecidos en el artículo 5 del RGPD y si las medidas de seguridad que se establezcan, en el caso que difieran de las fijadas en el ámbito del trabajo presencial, deberán ser cumplidas por el personal que desarrolle su trabajo bajo esta modalidad.

---

#### *4.- ¿Cómo proteger la información de la empresa y sus activos?*

---

La empresa debe velar por la protección de la información implementando un conjunto de medidas preventivas y reactivas. Estas medidas se establecerán en las correspondientes políticas: la Política de Seguridad de la Información orientada a cumplir con los principios de privacidad garantizando la disponibilidad, integridad y confidencialidad de la información; la Política de Ciberseguridad, cuyo objetivo será asegurar las conexiones y la autenticación en los sistemas, así como la actualización de firewalls y antivirus en todos los dispositivos y la Política de Teletrabajo, que describirá cómo debe ser el acceso remoto a la empresa, determinará los dispositivos válidos y canales de comunicación autorizados y establecerá un procedimiento para comunicar posibles incidentes, un protocolo para realizar videoconferencias o reuniones virtuales y la forma de actuar en caso de recibir un correo sospechoso, así como determinará las obligaciones y responsabilidades de la empresa y del empleado.

---

### *5.- ¿Cómo evitar riesgos de privacidad y seguridad en el marco del teletrabajo?*

---

Ya en 2017, el Grupo de Trabajo del artículo 29 de la Directiva Comunitaria 93/46/CE, sobre la protección de las personas físicas en lo relativo a la protección de datos personales, en su Dictamen 2/2017, advertía que el trabajo a distancia suponía un riesgo adicional para los derechos y libertades de los titulares de los datos personales, trabajadores y personas físicas cuyos datos son objeto de tratamiento por el Responsable y por ende por los trabajadores de ese Responsable.

En dicha Opinión, se ponía de relieve la necesidad de que la empresa realizase un análisis de los riesgos que implica para la protección de datos trabajar a distancia, al producirse una modificación en la forma de trabajar, la ubicación y en los medios utilizados, para establecer las medidas técnicas y organizativas necesarias.

Este análisis de riesgos, de acuerdo con lo dispuesto en el artículo 24 del RGPD, es obligatorio que se lleve a efecto. En este sentido la Agencia Española de Protección de Datos (AEPD) ha publicado guías para ayudar a los Responsables del Tratamiento, tanto a realizar ese análisis de riesgos como para establecer medidas técnicas y organizativas concretas. <https://www.aepd.es/sites/default/files/2020-04/nota-tecnica-proteger-datos-teletrabajo.pdf>

---

### *6.- ¿Cómo determinar las medidas de seguridad, técnicas y organizativas a implantar por la empresa?*

---

El artículo 32 del RGPD exige al responsable de los datos evaluar los riesgos inherentes al tratamiento de datos que pretende realizar y aplicar medidas para mitigarlos. En el caso de la empresa privada esta evaluación del riesgo podrá realizarse siguiendo estándares de seguridad existentes en el mercado como la norma ISO 27001. Por otro lado, para seleccionar las medidas a implementarlas con el fin de evitar la pérdida, alteración o acceso no autorizado a la información, las Administraciones Públicas deberán utilizar el Esquema Nacional de Seguridad.

En todo caso, será necesario implantar controles periódicos para verificar que las medidas tomadas siguen siendo efectivas y, en su caso, adoptar las medidas correctoras necesarias para garantizar la protección de la información.

## Eje 2 - Riesgos laborales y psicosociales y ergonomía

---

*1.- ¿Cómo puede la empresa cumplir con su obligación de evaluar los riesgos del puesto de trabajo remoto (psicosociales, físicos o ergonómicos) del personal teletrabajador desde el domicilio particular o desde centros de smart-working o co-working frente a la inviolabilidad del domicilio particular de éste o la gestión cruzada que pueda suponer con esos centros?*

---

Se puede cumplir recogiendo explícitamente el consentimiento del trabajador en el acuerdo de teletrabajo para su autoevaluación mediante declaraciones responsables y *checklists* facilitadas por el servicio de prevención de riesgos laborales de la empresa e, incluso, permitiendo el acceso a la zona de teletrabajo de su domicilio para su inspección “in situ” y recogiendo la obligación de informar de posibles centros admitidos por la empresa y concertados para teletrabajar, en los que se efectuará una coordinación de actividades empresariales. Adicionalmente, puede proveerle de herramientas de autoevaluación del puesto de trabajo, cuando así lo prefiera el empleado, en cuyo caso dicha información podría ser usada para corregir las deficiencias si las hubiera.

*2.- ¿Tienen las empresas un servicio de tutela, formación o ayuda al trabajador donde orientarle, formarle, aconsejarle y recibir sus necesidades o dudas para cubrir mejor los diferentes riesgos laborales?*

---

La empresa debería contar con un servicio que forme, tutele y enseñe a analizar los riesgos a los trabajadores de toda índole en su puesto de trabajo remoto, para poder realizar evaluaciones periódicas, y que les ayude en todas sus dudas y posibles cuestiones, incluso atienda necesidades, sugerencias o quejas. El acceso a dicho servicio debería ser sencillo y claro y el mismo debería proveer de formación adecuada en todo lo referente a ergonomía.

*3.- ¿Existen políticas de empresa que regulen el teletrabajo y todos y cada uno de sus aspectos, tales como responsabilidades mutuas, posibles accidentes en el domicilio, costes de las infraestructuras y necesidades del puesto de trabajo, monitorización de la actividad, ciberseguridad de datos y empleados, etc.?*

---

Los diferentes aspectos que es necesario cubrir en el acuerdo de teletrabajo deberían estar recogidos en una política de empresa, que respete lo dispuesto en cada convenio colectivo y esté debidamente consensuada con los representantes de los trabajadores, aprobada y comunicada a todas las partes que intervengan en el mismo. Debe dejar claras las responsabilidades de cada parte, las posibles acciones a llevar a cabo por la empresa, las monitorizaciones y controles, cómo actuar en todo momento, los costes asumidos, etc.



---

*4. ¿Existen procesos de inclusión y trabajo en equipo, que eviten el posible desapego del trabajador o sentimientos de exclusión, jornadas presenciales y/o actividades grupales?*

---

Con el fin de evitar posibles riesgos psicosociales en los trabajadores con sensación de exclusión, desapego, falta de sentido de equipo o de pertenencia a la organización, que como consecuencia pueden afectar a su salud, a su productividad y a posibles errores, la empresa debería proponer actividades grupales, de cohesión, de motivación y liderazgo por parte de los mandos y dirigidos a su equipo. La tecnología puede ayudar detectando patrones de trabajo que reflejen el *burn-out* del empleado, proveyendo de entornos seguros de trabajo en modo *Zero Trust* y facilitando el trabajo en equipo y la interacción mediante herramientas del metaverso.

Se requiere prestar una especial atención a los trabajadores de reciente incorporación en la empresa, para facilitar su inclusión en la cultura de la organización, y a teletrabajadores que viven solos, a quienes la falta de asistencia a la oficina puede impactar negativamente.

---

*5.- ¿Dispone la empresa de canales de denuncia y/o buzones de sugerencias y mejoras para recoger de forma segura y privada solicitudes, quejas o propuestas que mejoren el teletrabajo o eviten abusos y que permitan la gestión de posibles accidentes en el puesto remoto o domicilio del trabajador considerado como centro de trabajo adscrito?*

---

Ante la adopción masiva del teletrabajo como herramienta en cualquiera de sus formatos, tanto para conciliación, flexibilidad e incluso retención y atracción de talento, es necesario dotar de los mecanismos seguros y confidenciales para poder gestionar posibles accidentes, sugerencias, quejas, denuncias, etc. Es importante que, además del servicio de prevención de riesgos laborales de la empresa, participen otras áreas como recursos humanos, *compliance* y legal.

---

*6.- ¿Se preocupa la empresa de investigar y aplicar las best practices, políticas y mecanismos que garanticen mejor la conciliación de la vida privada y del trabajo, la desconexión digital, el trabajo por objetivos vs horarios rígidos o posibles abusos por parte de mandos o empleados?*

---

Esta modalidad de trabajo, el teletrabajo, supone un reto para la empresa y los trabajadores, en especial en estas cuestiones, y es por ello que la empresa debe ser exquisita en cubrirlas y atenderlas aplicando un proceso de transformación y las mejores prácticas en cada uno de los temas comentados. La tecnología debe poder facilitar la correcta aplicación del derecho a la desconexión digital, mediante la detección de patrones abusivos de trabajo para que estos puedan ser corregidos.

## Eje 3 - Infraestructura y riesgos de ciberseguridad

---

*1.- ¿Está preparada la red en España (tanto datos fijos como móviles) para soportar un cambio de forma de trabajo y que el teletrabajo (puro o híbrido) no haga perder eficiencia y productividad a las empresas?*

---

Se ha superado con nota la exigencia del teletrabajo y buena parte de eso la tiene que España es el primer país europeo en conexiones de fibra óptica, con una cobertura del 80% del territorio nacional. Algo similar ocurre con la red de datos de móviles, en los que el despliegue paulatino de las redes 5G incrementa el número de conexiones y la velocidad de las mismas. A través de la información ofrecida por DIRCE (fuente que valida la creciente densidad empresarial de las grandes ciudades y municipios del país según los datos disponibles), se puede constatar cómo el teletrabajo se ha beneficiado de una clara sinergia entre las prioridades de las empresas de telecomunicaciones a la hora de desplegar nuevas infraestructuras y la creciente densidad empresarial de las grandes ciudades y municipios del país. No obstante, sigue existiendo un área de oportunidad para acelerar los despliegues de redes fijas (fibra) y móviles (5G) en las regiones menos pobladas del país, donde el tejido empresarial está compuesto por pequeñas y medianas empresas.

La estrategia España Digital 2025, entre otras, persigue entre sus objetivos estratégicos mejorar la conectividad digital, garantizando un nivel adecuado para toda la población, y promoviendo la desaparición de la brecha digital entre zonas rurales y urbanas con el objetivo de que el 100% de la población tenga cobertura de 100 Mbps en 2025, y liderar el despliegue de la tecnología 5G en Europa, incentivando su contribución al aumento de la productividad económica, al progreso social y a la vertebración territorial. Se fija como objetivo que en 2025 el 100% del espectro radioeléctrico esté preparado para el 5G.

---

*2.- ¿Es suficiente el nivel de concienciación de los responsables de TI de las empresas para llevar a cabo las inversiones necesarias con el objetivo de cubrir al máximo posible las potenciales brechas de seguridad?*

---

Son de dominio público los casos de ataques de *malware* tanto en empresas como en organismos públicos. La publicidad de estos casos ha conseguido que se sea cada vez más consciente de los riesgos adicionales de seguridad que ha traído el teletrabajo, preocupación que es compartida por la dirección de las empresas. Todo ello ha posibilitado el incremento de las inversiones necesarias. Es cierto, pero muchas organizaciones esperan a sufrir un incidente antes de establecer medidas suficientes. La cuestión es si se ha avanzado lo suficiente intentando anticiparse al problema.

---

### *3. ¿Cuáles son las principales medidas y cambios a realizar en relación con las infraestructuras de seguridad, la operación de la seguridad, la gestión de la seguridad y las tareas responsables de seguridad?*

---

La principal medida es precisamente la integración de las diferentes estrategias de seguridad en un solo modelo denominado Cybersecurity Mesh, basado en una gestión y orquestación centralizada de políticas de seguridad, junto al uso de analíticas de datos e inteligencia artificial para la detección temprana de riesgos y su correspondiente gestión de identidad distribuida.

En gran parte de las organizaciones y empresas se contemplan medidas más tradicionales de seguridad para segmentar las redes, contar con una red interna vigilada, mantener una política de contraseñas robusta, evitar sistemas obsoletos y sin actualizaciones de seguridad, contar con suficiente personal de seguridad TI que posee la adecuada cualificación técnica, contar con *backup* desconectado de la red, gestionar los accesos remotos con doble factor de autenticación, controlar a los administradores locales, establecer suficiente nivel de auditoría (logs no muy limitados en el tiempo), asegurar una monitorización continua, controlar también las redes de confianza, contar con protección EDR (Endpoint Detection Response) y gestionar y controlar los privilegios en dispositivos de Internet de las Cosas.

Es recomendable el uso de productos confiables y certificados, la concienciación de los usuarios, el compromiso de la dirección y la compartición de buenas prácticas. Además, es importante establecer procesos para modificar la cultura de la organización, incluyendo la concienciación de todos los empleados, especialmente los altos directivos o los altos cargos.

En cuanto a las Administraciones Públicas, estas cuentan con el Esquema Nacional de Seguridad y con las guías CCN TIC.

---

### *4.- ¿Qué medidas específicas se requieren para permitir políticas de BYOD (Bring Your Own Device)?*

---

Si bien el BYOD introduce la experiencia de casa en el trabajo, su implantación implica riesgos adicionales de seguridad y un modelo de gestión más complejo. Para su correcta implantación es necesario definir un equipo de trabajo que se enfoque en analizar el estado del riesgo de los dispositivos personales, establecer qué objetivos se quieren cubrir mediante el uso de BYOD y desarrollar un plan de consecución de dichos objetivos exponiendo claramente los riesgos a los que se somete la organización. Es necesario asegurar la concienciación y formación de todos los empleados en materia de seguridad y contar con las herramientas de ciberseguridad necesarias (autenticaciones, firewalls, túneles, MDMs...).

El empleo del modelo de seguridad *Zero Trust*, compatible con la implementación del acceso con mínimo privilegio, facilita el uso de los dispositivos BYOD.

Desde un punto de vista legal, debe tenerse en cuenta en todo caso que la obligación de proveer las herramientas de trabajo es del empresario, por lo que habría que regular bien en el acuerdo de trabajo a distancia en qué condiciones van a poner los empleados sus propios medios.

---

*5.- ¿Qué modelo de seguridad es más efectivo en el teletrabajo?*

---

El modelo de seguridad más efectivo es el Zero Trust. Nunca hay que asumir que el usuario que se identifica con su *password* es quien dice ser. La implementación de medidas como la verificación en dos pasos o la detección inteligente basada en geolocalización y comportamientos se debe incluir en la base del teletrabajo. En este modelo desaparecen los perímetros de seguridad y se incorporan variables adicionales para autenticar y autorizar SIEMPRE el acceso a los recursos de la organización: además de la identidad, reforzada con factores de doble autenticación, se tiene en cuenta el contexto en que se solicita el acceso (por ejemplo el tipo de dispositivo -smartphone, portátil, etc.-, el sistema operativo y su nivel de actualización, el tipo de red -fija o móvil-, el lugar de acceso -oficina, casa o red pública-, la hora -horas laborales o extralaborales- o la periodicidad de las solicitudes -recurrente, nueva solicitud, etc.-).

Adicionalmente al Zero Trust, es necesario contar con servicios que encripten las comunicaciones como son los *Idata Tunnel*, que permiten establecer conexiones remotas a la VPN de la empresa mediante túneles encriptados y a través de cualquier conexión a Internet. Ofrecen conexiones seguras a la VPN, desde el dispositivo PC o el laptop contra el *router* gestionado por los diferentes ISPs.

---

*6.- ¿Las soluciones de ciberseguridad implementadas para el teletrabajo permiten un acceso eficaz del trabajador a los recursos y aplicaciones que utiliza normalmente, con la misma funcionalidad completa y los mismos procedimientos de acceso, o limitan la funcionalidad y hacen complejo el procedimiento de acceso? ¿Existe un perfil especial de ciberseguridad según la criticidad de los recursos?*

---

Las soluciones de ciberseguridad correctamente implementadas permiten el acceso a los recursos y aplicaciones necesarias para el adecuado desempeño del trabajo del empleado y lo hacen de manera transparente, de modo que no sea distinguible el acceso por localización. Si bien es verdad que muchas veces las conexiones domésticas o públicas que se pueden utilizar para el teletrabajo no son tan potentes como las corporativas (especialmente en las grandes empresas) y si, además, se suma la necesidad de contar con elementos de ciberseguridad en ciertas situaciones, algunas acciones pueden tardar más en ejecutarse conllevando una pérdida de productividad.

---

*7.- ¿Hay una estrategia de movilidad empresarial bien definida e integrada con la estrategia TI global de la empresa?*

---

La realidad es que ese tipo de estrategias se ha acelerado gracias a la pandemia y a la adopción forzosa del teletrabajo. En los primeros meses de pandemia fue una necesidad que los empleados pudieran trabajar de manera remota. En este momento se ha adoptado, por muchas empresas, un modelo híbrido que la mayoría de compañías incluyen en su estrategia empresarial como beneficio.

## Eje 4 - Cultura: concienciación, formación y capacitación

---

*1.- ¿Está una empresa preparada o tiene reticencias para la implantación del teletrabajo y sus diferentes modelos? ¿Conocen los grupos de interés de la empresa la implicación del teletrabajo? ¿Quién debe liderar la iniciativa de adoptarlo mediante la definición y adopción de una estrategia?*

---

Para la implantación del teletrabajo, es importante considerar que hay una relación entre la motivación del empleado y su productividad y que una forma de impulsar la motivación es favorecer la conciliación de la vida laboral y personal. También hay que estar dispuesto a abordar algunos cambios organizativos. A partir de ahí, sería necesario consensuar entre las partes las necesidades mínimas a nivel de recursos humanos, representación de los trabajadores, sondeo a empleados, etc. Con ello es posible definir la estrategia y el alcance del teletrabajo y un plan completo de adopción y comunicación.

---

*2.- ¿Se debe disponer de una Política Organizacional para el teletrabajo con todo su desarrollo de normas y procedimientos, así como de roles y responsabilidades, puestos que pueden adoptarlo, modos de teletrabajo y tipos de conexión remota aceptados y marco legal y de compliance aprobado en la organización?*

---

Es necesario atenerse a los marcos legales y regulatorios que tratan el teletrabajo y trasponerlos dentro de los roles, puestos y procesos y servicios de la organización mediante un marco que lo regule, aprobado por la dirección y por representantes de los trabajadores y áreas de recursos humanos, *compliance*, legal y riesgos laborales, así como por las áreas de seguridad y ciberseguridad.

---

*3.- ¿Cuentan la organización y los trabajadores con los medios (infraestructuras, dispositivos, plataformas o aplicaciones) y los servicios necesarios para poder establecer sistemas de teletrabajo desde el domicilio o desde centros de smart-working o co-working?*

---

Es aconsejable evaluar necesidades de tipos de puestos, políticas de dispositivos a utilizar (BYOD o solo empresa), herramientas de conectividad aceptadas para un uso seguro y confidencial, comunicaciones en cada caso, equipamientos en el puesto remoto, riesgos laborales, etc. Así como disponer de un centro de ayuda y soporte al trabajador para configurar y resolver dudas, de un cuerpo de FAQs y de trípticos, decálogos, manuales, formularios, aplicaciones, etc.

---

*4.- ¿Dispone la organización de servicios propios o ajenos para crear la suficiente y adecuada concienciación, formación y capacitación de todos los roles y perfiles que vayan a teletrabajar y de los que puedan dar soporte a los mismos? En definitiva, ¿dispone de la cultura necesaria en todos y cada uno de los aspectos legales y de compliance, privacidad, técnicos o de uso, así como de sus derechos y obligaciones, formalización, responsabilidades, privacidad y ciberseguridad, rutinas, espacio de trabajo definido, desconexión digital, objetivos, procedimientos, etc.?*

---

La organización debe definir una estrategia y unos planes de acción que serán comunicados a todos los implicados para hacerles partícipes de los objetivos, procedimientos y protocolos que favorezcan el mejor desempeño del trabajo y la productividad. Asimismo, es necesario implementar las herramientas que faciliten la transmisión de conocimientos, el control de objetivos, la colaboración entre equipos y la definición de itinerarios formativos. Será clave la homogeneización de los procedimientos y buenas prácticas en el teletrabajo. Resulta totalmente necesaria la concienciación en materia de ciberseguridad, al aumentarse la superficie de exposición y el riesgo de materialización de ciberataques.

Los planes de actuación, procedimientos y protocolos serán revisados periódicamente para adaptarlos a las novedades que aparezcan. Habría que destacar la importancia de cubrir las necesidades de las nuevas incorporaciones de empleados, por lo que es conveniente diseñar un pack de bienvenida y un protocolo de acompañamiento que haga progresiva la incorporación a sus nuevas responsabilidades.

---

*5.- ¿Hay que elaborar un plan de comunicación específico para concienciar sobre los aspectos del teletrabajo (objetivo, nuevos procedimientos, nuevos métodos de reporting, nuevas herramientas, utilización eficaz de las herramientas, riesgos, ventajas, conciliación, desconexión digital, formación y soporte disponible, etc.)?*

---

Una vez definida la estrategia, los procedimientos, los protocolos, las herramientas y las buenas prácticas es conveniente establecer un buen plan de comunicación a todos los niveles para garantizar la mejor gestión del proceso de cambio. Es importante combinarlo con los recursos e itinerarios formativos y con otras actividades para dar a conocer todos los procedimientos necesarios para establecer una colaboración fluida y homogénea. Se deben reflejar los principales casos de uso para mejorar la comprensión y acercar el modelo a los empleados.

El plan de comunicación apoya la gestión del proceso de cambio del método de trabajo, la adopción por parte de todas las partes y la contribución que exige a la nueva cultura, ayudando a minimizar posibles desigualdades, malos hábitos o usos, a conseguir una más rápida adopción y a reducir incidentes o problemas. Para evitar desigualdades y el rechazo a este modelo de trabajo es necesario realizar un acompañamiento en aquellos colectivos con menor formación o recursos y en el caso de colectivos específicos. Es conveniente realizar encuestas de satisfacción para ir adaptando y mejorando procedimientos y herramientas.

---

*6.- ¿Cómo puede el teletrabajo aumentar el vínculo y generar confianza entre la empresa, los mandos y el trabajador, tanto para evitar desigualdades, incluida la cuestión de género, como para potenciar actividades de cohesión de equipos o analizar cómo impacta en el cambio de liderazgo de equipos y qué nuevas habilidades son necesarias para ello?*

---

La desconexión física y social entre personas que implica el teletrabajo podría desembocar en un menor vínculo de los trabajadores con la empresa y su cultura si no se cuida este aspecto. Por tanto, es imprescindible promover actividades de cohesión, nuevas técnicas de liderazgo y mucha empatía por parte de los responsables de la empresa para, no solo evitar el riesgo, sino reforzar el vínculo empresarial cuidando de todos los aspectos que puedan llegar a afectar a una persona, evitando posibles desigualdades, aislamientos sociales, riesgos para la salud del trabajador, y por ende de su productividad, así como la disminución del sentido de pertenencia al equipo y a la organización.



## Eje 5 - Productividad y negocio

---

### 1.- ¿La productividad aumenta en el teletrabajo?

---

Existen diversos estudios que revelan como el trabajo híbrido o incluso el teletrabajo aumentan la productividad como son:

- “*Un lugar de trabajo sostenible: hacia un modelo remoto y presencial*”, del IESE y Savills Aguirre Newman.
- Informe de la consultora estadounidense Omdia para su estudio sobre el futuro del trabajo.
- Informe de la Universidad de Stanford (Estados Unidos) “*Does working from home work?*”.

Las principales razones por las que se aumenta la productividad y en la que coinciden la mayoría de ellos son:

- Ahorro del tiempo de desplazamiento a la oficina.
- Flexibilidad en el trabajo.
- Mayor dedicación de horas.
- Mayor capacidad de concentración y menor número de distracciones, que aumentan la productividad por minuto.
- Ambiente cómodo y relajado.
- Menor número de reuniones.
- Mayor autonomía.
- Pausas más cortas.
- Menor número de días de ausencia por enfermedad.

En general los teletrabajadores muestran mayor satisfacción en sus puestos de trabajo y mayor compromiso con la empresa. Además de ser uno de los factores que incrementa la retención del talento y es decisivo a la hora de tomar en consideración un nuevo empleo.

---

### 2. - ¿Cómo medir la productividad?

---

El modelo ha cambiado y tiende a la desaparición de las técnicas de presencialismo. El acudir a la oficina está enfocado a la colaboración y supone un lugar de encuentro para la co-creación, más que a tener que ir porque sí.

Para poder medir la productividad se requiere mejorar la comunicación y:

- Establecer objetivos y metas y cómo conseguirlos.
- Delegar y fijar en quién.
- Establecer rutinas y procedimientos.
- Crear hitos y celebrar su consecución.
- Considerar que la comunicación y la transparencia son fundamentales.
- Diseñar tareas y procesos claros y comprensibles.



La medición de la productividad se puede hacer:

- Estableciendo objetivos, pactándolos y supervisándolos.
- Implementando un sistema de flujo de actividad.

Se deben seleccionar indicadores objetivos de productividad (KPIs o mejor KPS utilizando objetivos *smart*), alineados con el trabajo por objetivos y enfocados al resultado. Y, por último, es necesario contar con las herramientas adecuadas que favorezcan este seguimiento y evaluación continuos.

---

### *3. ¿Promueve el teletrabajo la creatividad, favorece la optimización del tiempo y disminuye los conflictos entre los miembros de la empresa?*

---

La creatividad e innovación necesitan tanto del trabajo en equipo como del trabajo en solitario, por lo que el modelo híbrido puede ser perfecto para conseguir equipos más creativos e innovadores. En cualquier caso, es beneficioso fomentar la compartición de ideas y establecer espacios de colaboración presenciales y virtuales.

La optimización del tiempo en la modalidad de teletrabajo es fundamental. Se consigue definiendo los objetivos y metas y estructurando las jornadas.

También, al tener menor contacto presencial, los desacuerdos o dinámicas negativas que pueden surgir en un equipo disminuyen.

---

### *4.- ¿Cómo gestionar y alinear los equipos de trabajo hacia la consecución de los objetivos de negocio asignados al grupo en el teletrabajo?*

---

Conviene redefinir los procesos de reporte, coordinar las actividades del equipo y definir los objetivos y métricas para adaptarlos al nuevo contexto.

Además de las herramientas de videoconferencia y de las plataformas comerciales de uso generalizado para compartir información en la nube, existen herramientas diseñadas específicamente para el trabajo en equipo y la colaboración remota.

---

### *5.- ¿Se pueden reducir costes con el teletrabajo?*

---

Conviene realizar un análisis de costes de infraestructura, espacio de oficina y recursos necesarios. Si una parte de los trabajadores va a dejar de ir a la oficina durante periodos largos de tiempo, esto debería redundar en la reducción de espacio disponible, con la consiguiente reducción de costes. Se puede alternar el uso de espacios en la oficina entre distintos equipos de trabajo durante periodos de tiempo establecidos (el conocido como “sistema de mesas calientes”).

---

## *6.- ¿Puede el teletrabajo ayudar en el servicio al cliente?*

---

De dos maneras:

1. Si la interacción con el cliente es presencial, el agente de servicio o representante comercial se desplazará directamente desde su domicilio a la ubicación del cliente, ahorrándose así el trayecto domicilio-oficina.
2. Si la interacción con el cliente es remota, debe disponer en su puesto de trabajo remoto de todas las herramientas necesarias para la prestación del servicio con el nivel de calidad requerido. Así consigue mayor flexibilidad en horarios, más tiempo con el cliente y una mejora en la conciliación, al ahorrarse el tiempo de los desplazamientos.

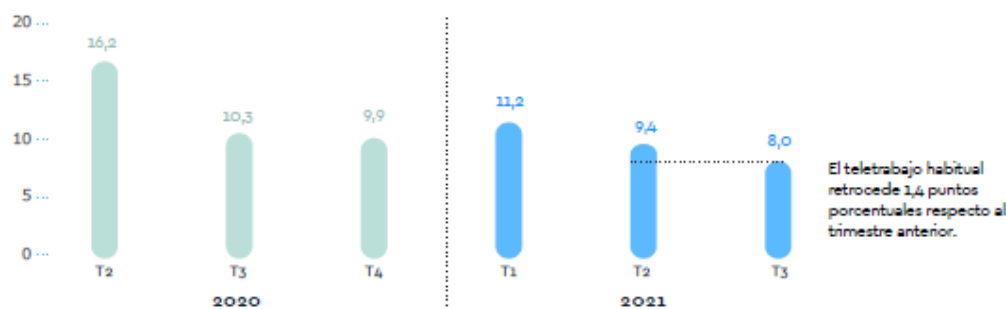
## Anexo - Algunos datos sobre teletrabajo

### La evolución del teletrabajo en España

Aunque el teletrabajo ya era una tendencia creciente en los últimos años, ha sido con la pandemia de la COVID-19 cuando su protagonismo se ha multiplicado de forma evidente. La crisis sanitaria ha tenido un impacto disruptivo en los mercados laborales de todo el mundo durante 2020, y en menor medida en 2021, y muchos trabajadores se han visto obligados a adaptarse de forma acelerada a realizar las labores profesionales desde sus domicilios al cerrar las oficinas y otros centros de trabajo.

En el caso español, y con datos de la Encuesta de Población Activa (EPA) del INE, recogidos por el ONTSI<sup>1</sup>, se observa un pico en la cifra de teletrabajadores habituales (que han teletrabajado en su propio domicilio más de la mitad de los días) en el segundo trimestre de 2020 del 16,2%. Este porcentaje ha ido variando en los siguientes trimestres en función de las olas de la pandemia, pero con una tendencia a la baja. En el tercer trimestre de 2021, ese porcentaje ha sido del 8% de los españoles ocupados, lo que supone casi 1,6 millones de personas. Ese porcentaje contrasta con el 9,4% del segundo trimestre de 2021 y con el 10,3% del tercer trimestre de 2020.

### Porcentaje de ocupados que han trabajado desde el domicilio particular habitualmente. España



*Fuente: Encuesta de Población Activa – EPA (INE), vía ONTSI.*

Los datos del cuarto trimestre reflejan una cierta estabilización del trabajo desde casa<sup>2</sup>. El 7,9% de los ocupados trabajó desde su propio domicilio más de la mitad de los días.

La evolución de las cifras muestra que en los últimos trimestres se está consolidando la vuelta al trabajo presencial, con los lógicos vaivenes debidos a las diferentes olas de la pandemia. La vacunación masiva de la población española ha ayudado a recuperar una cierta normalidad en la actividad económica y social y, con ella, a aumentar el nivel del trabajo presencial.

No obstante, lo que si se consolida es un incremento destacado del teletrabajo respecto a los valores anteriores al inicio de la pandemia. A finales de 2019, el porcentaje de teletrabajadores era del 4,8% de los españoles ocupados frente a alrededor del 8% en los últimos trimestres.

<sup>1</sup> “Flash datos de Teletrabajo. Tercer trimestre 2021”. ONTSI. 2021.

<sup>2</sup> “Encuesta de Población Activa (EPA). Cuarto trimestre de 2021”. INE. 2022.

## El punto de vista de las empresas y las Administraciones Públicas

Un análisis realizado por Vodafone<sup>3</sup> sobre el teletrabajo en España ofrece algunas pistas sobre las tendencias presentes y futuras desde la óptica de las empresas y de las Administraciones Públicas. En el caso de las empresas, a medida que aumenta el tamaño de las organizaciones crece el protagonismo del teletrabajo durante los meses de la pandemia. En un extremo se sitúan las grandes empresas, en las que la implantación del teletrabajo ha sido mayoritaria (94%), partiendo del hecho que ya contaban con porcentajes consolidados de teletrabajadores antes de la pandemia (50%). En el extremo opuesto, el teletrabajo en las microempresas se ha duplicado hasta alcanzar un limitado 30% durante los meses de un confinamiento más intenso. Las Administraciones Públicas, por su parte, han pasado de una implantación del teletrabajo antes de la pandemia del 18% a un máximo durante el confinamiento del 91%.

A corto plazo, el análisis muestra que todas las organizaciones planean reducir su nivel de teletrabajo, pero las empresas, sea cual sea su tamaño, estiman mantener niveles ligeramente superiores a la situación previa a la pandemia. Sin embargo, en el caso de las Administraciones Públicas el porcentaje de teletrabajadores podría estabilizarse en un 55%, lo que supondría un incremento notable respecto a la situación previa.

Desde la óptica de la preparación al teletrabajo, las empresas españolas consideran que disponían de las soluciones necesarias para la implementación de esta modalidad laboral durante la pandemia. La mayoría de las compañías se consideraban preparadas para el teletrabajo cuando se inició la crisis sanitaria, situándose a la cabeza de esta opinión las grandes empresas (87%) y las pymes (84%). Sin embargo, las Administraciones Públicas creen que han estado menos preparadas para hacer frente al teletrabajo durante la crisis de 2020.

## El punto de vista de los directivos

Un análisis realizado por McKinsey<sup>4</sup> a partir de los datos obtenidos en una encuesta a 100 directivos de empresas de diferentes sectores y zonas geográficas concluye que nueve de cada diez organizaciones van a combinar en trabajo presencial y el trabajo remoto en la etapa post pandemia de la COVID-19. El análisis también confirma que la productividad y la satisfacción de los clientes se han incrementado durante la pandemia, época en la que el teletrabajo ha alcanzado su pico más alto.

Otra de las conclusiones del trabajo de McKinsey es que en el futuro el trabajo será más híbrido de lo que lo era antes de la crisis sanitaria. Antes de la pandemia, la mayoría de las organizaciones basaban su estrategia en el trabajo presencial. Pero, cuando los efectos de la COVID-19 parecen disminuir, los directivos opinan que el trabajo híbrido será claramente más común. Esos mismos directivos señalan que, en los puestos de trabajo que no requieran obligatoriamente presencia física, los empleados trabajarán de forma presencial entre uno y cuatro días a la semana (dos o tres días como escenario más probable).

## El punto de vista de los trabajadores

Según los resultados de una encuesta de PwC realizada a trabajadores de 19 países<sup>5</sup> (entre ellos España) sobre sus expectativas y temores acerca del mercado laboral del futuro, los empleados lo tienen muy claro: para la vuelta a la normalidad después de la pandemia van a demandar una mayor flexibilidad laboral y apuestan por fórmulas híbridas entre lo presencial y lo

---

<sup>3</sup> “Observatorio Vodafone de la Empresa. IV Estudio sobre el Estado de Digitalización de las Empresas y Administraciones Públicas españolas”. Vodafone Business. 2021.

<sup>4</sup> “What executives are saying about the future of hybrid work”. McKinsey&Company. 2021.

<sup>5</sup> “2021 Hopes & Fears Survey”. PwC. 2021.

virtual. El 72% de los encuestados que han trabajado a distancia durante la pandemia prefiere una forma de trabajo híbrida, cifra que sube al 74% en España, mientras que al 19% le gustaría no volver a una oficina física y trabajar totalmente a distancia y solo el 9% demanda volver a trabajar como antes de la pandemia. Además, más de la mitad de los encuestados espera que el teletrabajo sea una parte permanente de la oferta laboral de sus empresas, que van a necesitar a partir de ahora diferentes tipos de espacios físicos.

En la misma línea, un análisis de Microsoft<sup>6</sup> con datos de 31 países muestra que los trabajadores quieren lo mejor de ambos mundos (virtual y presencial): el 73% pide que se mantengan las opciones de teletrabajo, mientras que el 67% anhela más tiempo de contacto personal y de colaboración presencial. Estas demandas y tendencias van a obligar a las compañías a rediseñar los espacios físicos para acomodar mejor los entornos de trabajo híbridos. En definitiva, los trabajadores piden niveles más elevados de flexibilidad y la implantación de modelos de trabajo híbrido, circunstancias que definirán los espacios de trabajo en la era post pandemia.

Finalmente, un informe realizado por el IESE y Savills Aguirre Newman<sup>7</sup>, mediante encuestas en 11 países, concluye que solo un 12% de los empleados trabajaría en remoto todos los días. De ellos, la mayoría son mujeres (64%). En el otro extremo se sitúan los no quieren teletrabajar nunca, que apenas representan un 4% de la muestra. El 54% de ellos asegura que prefiere trabajar de forma presencial para estar cerca de su equipo. Como resumen, la opción preferida por los empleados es trabajar desde casa tres días a la semana (36%), seguida de la opción de dos días semanales (32%). La edad no tiene un impacto significativo en estas preferencias.

---

<sup>6</sup> “2021 Work Trend Index: Annual Report. The Next Great Disruption Is Hybrid Work—Are We Ready?”. Microsoft. 2021.

<sup>7</sup> “Un lugar de trabajo sostenible: hacia un modelo remoto y presencial”. IESE y Savills Aguirre Newman. 2021.

## AUTORES

**Juanjo Martínez Pagán.** Presidente del Grupo de IT Digital de AUTELSI. Asesor de CISOs en nuevas brechas de seguridad. Mentor de startups de ciberseguridad. Fundador de ThousandGuards.

**Javier Asenjo.** Director de RRHH de NCR España. Scrum manager certified. Consultor y experto en RRHH y tecnología.

**Carmen Cabanillas Serrano.** Presidenta de ASTIC, Subdirectora General de Gobernanza en materia de registros, funcionaria del Cuerpo Superior de Sistemas y Tecnologías de la Administración de la Seguridad Social.

**Hugo Fernández Rodríguez.** Director General de WIZY en Iberia. Más de 15 años de experiencia en el desarrollo de negocio de tecnología y movilidad empresarial en Asia, Latinoamérica y Europa.

**Pedro Galián Úbeda.** Jefe de Ingeniería de Comunicaciones en Renfe. Lleva más de 25 años en el mundo de las Comunicaciones y la Seguridad. Actualmente es responsable del área de Ingeniería de Comunicaciones y Seguridad en el ámbito de los CPD y la red de datos.

**Fernando Goñi Ubieta.** Director Modern Workplace en DXC para España y Portugal. Más de 25 años de experiencia en áreas de Tecnología, Ingeniero Informático y MBA.

**Pedro Pablo López Bernal.** Presidente Continuum, Sigeco y Foro Resilium. Experto en Resiliencia, Continuidad, Ciberseguridad, Privacidad, Auditoría y Gobierno.

**Carlos López Goñi.** Director Financiero y Servicios Generales de Nasertic. Responsable de Recursos Humanos. Buscamos potenciar el talento y la productividad desde la conciliación.

**Clara Marín Hernández.** Directora en el Área Laboral de la oficina de Madrid del despacho Andersen. Abogada con 20 años de experiencia en el asesoramiento jurídico laboral integral a empresas multinacionales de diversos sectores.

**Carlos Maza Frechín.** Subdirector de Tecnologías de la Información y Comunicaciones. Ha desempeñado su labor profesional en el sector privado y en el público, en este último en los Ministerios de Hacienda, Economía e Industria y actualmente en el Tribunal de Cuentas.

**Javier Ordozgoiti Hernández.** 16 años en puestos de marketing y trade en sector gran consumo. En Vodafone lleva las cuentas High desde una posición de commercial manager. Actualmente gestiona IPVPN & Ciberseguridad en el departamento de marketing.

**José Miguel Roca Chillida.** Consultor en tecnologías digitales y su impacto económico y social y editor del blog InformeTICplus.com.

**Ernesto Ruiz de Galarreta-Arbeo.** Ingeniero de Telecomunicaciones y MBA. 20 años de experiencia internacional en consultoría tecnológica, desarrollo de negocio y ventas. Desde 2019 Director de Tecnologías de la Información en Nasertic.

**María Suárez Pliego.** Socia en el despacho de abogados Andersen en el área de Privacidad, Propiedad Intelectual y Tecnologías de la Información. Trabaja asesorando, en el ámbito internacional, a empresas del sector de tecnología.

**Leonor Torres Moreno.** Vicepresidenta de ASTIC, Jefa de servicio de Informática del Ayuntamiento de Madrid. Funcionaria del Cuerpo Superior de Sistemas y Tecnologías de la Administración de la Seguridad Social.

**Silvia Tortosa Méndez.** DPO en DXC Technology para España y Portugal desde 2019. Licenciada en Derecho con más de 20 años de experiencia en el entorno de la Gestión de la Seguridad de la Información y Privacidad.