DIPUTACIÓ DE VALÈNCIA

Protecció de Dades i Seguretat de la Informació

Boletín protección de datos

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

Boletín N.º 2| Agosto 2020

PLATAFORMAS Y APLICACIONES EN EL TELETRABAJO

Í N D I C E

Pág

Tema central

Plataformas y aplicaciones en el teletrabajo 2-6

Material complementario 7

• Recomendaciones de la AEPD para proteger los datos personales en situaciones de movilidad y teletrabajo.

• Recomendaciones de Seguridad para situaciones de teletrabajo y refuerzo en vigilancia

• Anteproyecto de ley de Trabajo a Distancia

Noticias de actualidad 7

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

SUSCRIPCIONES

Si deseas suscribirse a nuestro Boletín informativo accede al siguiente enlace

PLATAFORMAS Y APLICACIONES EN EL TELETRABAJO

Parece que el teletrabajo ha venido para quedarse, no sólo como circunstancia sobrevenida, ya que como indicamos en el boletín anterior, desde el Ministerio de Trabajo se ha elaborado un anteproyecto de ley, presentado el pasado 26 de junio, para regular el empleo a distancia. Algunas de las cuestiones que aborda son la voluntariedad de escoger esta forma de trabajar, **el reparto de costes, la desconexión digital o el horario**, ocasionando que el mercado laboral en España pasa por impulsar definitivamente la instauración del teletrabajo.

Con motivo del cambio de perspectiva al que nos estamos enfrentado, dada la imposibilidad de desarrollar los servicios de forma presencial, ha sido necesario adaptar nuestra metodología de trabajo a un sistema digital. Por ello, el presente boletín atiende a la necesidad de búsqueda de alternativas para continuar con la prestación de la actividad de manera efectiva, sin olvidar el cumplimiento del marco jurídico que debe encuadrarse en el desarrollo de nuestra actividad.

Vamos a ver algunas de las cuestiones a tener en cuenta para que la **implementación de un sistema digitalizado se desarrolle sin riesgos jurídicos, esclareciendo una serie de aspectos que tanto empleador como empleado** deben de tener en cuenta para establecer una buena estrategia de teletrabajo.

Supuestos de aplicación

El desarrollo de la adecuada implementación del trabajo a través de modalidades a distancia y online puede implicar la necesidad de:

- **Utilización de aplicaciones para desarrollar reuniones** de forma telemática a través de videoconferencia (Skype, Google Hangouts, Webex, Teams y Zoom)
- Utilización de **herramientas de almacenamiento en nube** (tipo Dropbox, Google Drive, OneDrive, etc.)
- Utilización de **correo electrónico** para el intercambio de información entre trabajadores

Tratamiento de datos personales en internet

Hoy día hemos visto que la necesidad de atender a situaciones como la que nos encontramos actualmente, supone que las entidades hayan recurrido a las soluciones que facilitan las tecnologías de la información y comunicación, en particular al uso de servicios de *cloud computing* o de computación en nube y aplicaciones para desarrollar reuniones de forma telemática a través de videoconferencia.

En estos supuestos es esencial atender a las obligaciones derivadas de la normativa aplicable en materia de protección de datos, analizando las implicaciones que plantean el uso de dichas plataformas.

En este sentido, la entidad deberá disponer de la información claramente definida sobre los tratamientos efectuados, las finalidades de los mismos y sus responsables, así como sobre la ubicación de los datos, el periodo de retención, y las garantías con relación a su seguridad, que ofrecen dichas plataformas

"La entidad deberá disponer de la información claramente definida sobre los tratamientos efectuados, las finalidades de los mismos y sus responsables, así como sobre la ubicación de los datos, el periodo de retención, y las garantías con relación a su seguridad, que ofrecen dichas plataformas"

ORIENTACIONES PARA LA EVALUACIÓN DE APLICACIONES

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 garantizar que los empleados conozcan una serie de buenas prácticas en el desempeño de sus funciones:

A) Sobre la información ofrecida por los responsables de la aplicación

Se debe comprobar si el responsable de la aplicación informa claramente de los siguientes:

- la identidad y dirección del responsable,
- las finalidades para las que serán utilizados los datos,
- las posibles comunicaciones de datos a terceros y su identidad, así como la finalidad para la que se ceden,
- los derechos que asisten a los titulares de los datos,
- la ubicación de los datos y sus periodos de conservación,
- las medidas de seguridad facilitadas por la aplicación,
- los posibles accesos que realiza la aplicación a los datos personales almacenados en el dispositivo o a sus sensores.

Esta información debería estar fácilmente accesible en la **política de seguridad** de la aplicación. En caso de que falte alguno de estos aspectos, o que la información facilitada no ofrezca las garantías adecuadas, se recomienda no utilizar la aplicación.

B) Sobre la ubicación de los datos

Los datos deben estar almacenados en un **país del Espacio Económico Europeo o un país que ofrezca un nivel de protección equivalente** (que haya sido así acordado por la Agencia Española de Protección de Datos o por Decisión de la Comisión Europea).

Puede consultar la lista de países con nivel adecuado de protección en el siguiente enlace.

En cualquier otro caso, se recomienda solicitar información sobre las posibles transferencias internacionales de datos y las garantías de su licitud, en particular sobre las que necesitan autorización por parte de la Agencia Española de Protección de Datos.

> ***""La responsabilidad del cumplimiento de las medidas de seguridad debe entenderse siempre compartida entre los diferentes actores intervinientes (responsable de la aplicación, la entidad y los usuarios)"***

C) Sobre la seguridad de los datos

La responsabilidad del cumplimiento de las medidas de seguridad debe entenderse **siempre compartida** entre los diferentes actores intervinientes (responsable de la aplicación, la entidad y los usuarios), debiendo en todo caso el responsable de la aplicación facilitar las medidas técnicas adecuadas para garantizar la seguridad de los datos tratados, y la entidad aplicarlas o utilizarlas correctamente, además de implementar las medidas organizativas apropiadas.

La responsabilidad de las **medidas de identificación** de usuarios también es compartida. Por un lado, la aplicación debe implementar un mecanismo de autenticación que permita la identificación inequívoca y personalizada de los usuarios, recomendándose que este mecanismo consista en códigos de usuario y contraseñas, evitando la identificación mediante datos biométricos (reconocimiento facial o huella dactilar).

Si se utilizan contraseñas, la entidad debe incluir en su política el cambio periódico de las mismas, por lo que las aplicaciones que se vayan a utilizar deben incluir mecanismos para permitir dichos cambios. A los usuarios les corresponde la obligación de utilizar de **contraseñas robustas y custodiarlas sin desvelarlas a terceros**.

D) Prueba de la aplicación

Se considera conveniente poner a prueba la aplicación de forma previa a su definitiva utilización en la entidad, realizando la prueba sin introducir datos personales reales en su utilización. En esta fase de prueba se debería comprobar la corrección de las informaciones que fueron facilitadas por el responsable de la aplicación.

E) Documentación de la evaluación

Se recomienda documentar las evaluaciones realizadas dejando constancia de los aspectos que han sido analizados y de los resultados obtenidos

APLICACIONES CONCRETAS

Skype

Skype es una de las pioneras de esta lista de aplicaciones ya que su lanzamiento se produjo en el año 2003. Fue creado como un servicio Voz-sobre-IP (VoIP), es decir, transmisiones de voz a través de Internet utilizando una webcam y un micrófono para ordenador, poco a poco Skype fue añadiendo las funciones que conocemos hoy día: la mensajería instantánea mediante texto, las videoconferencias, los videomensajes, las llamadas a teléfonos convencionales, o el intercambio de información.

Su avance propició el salto a otros sistemas operativos y dispositivos como las consolas o las Smart TV, y ha sustentado a las videollamadas de la red social Facebook. Actualmente cuenta con las características que contienen el resto de aplicaciones, conecta a los usuarios vía texto (mensajería instantánea), voz (VoIP) o vídeo desde y hacia cualquier punto del mundo. También permite realizar llamadas entre ordenadores y la red de telefonía fija o móvil. Se puede acceder tanto desde el Smartphone como desde un PC.

A continuación, indicamos algunas de las cuestiones que pueden resultar más relevantes en materia de protección de datos y seguridad de la información en el uso de esta plataforma:

- Privacidad y Seguridad en Skype
- ¿Cuánto tiempo permanecen los archivos y datos disponibles en Skype?
- Declaración de privacidad de Microsoft

Hangouts de Google

Hangouts es una aplicación de mensajería instantánea, llamadas telefónicas y de videoconferencia, y es una funcionalidad que está incluida dentro de la plataforma Google +. Surgió en 2013 para entrar a competir junto con Skype, con la ventaja en aquel momento de permitir hacer llamadas, con voz o con video, a 10 personas simultáneamente. Además, permitía hacer charlas públicas y cualquiera podía acceder a ellas desde un enlace.

Actualmente, cuenta con las características comunes al resto de estas herramientas, permitiendo la comunicación entre los usuarios vía texto (mensajería instantánea), voz (VoIP) o vídeo y desde cualquier parte. Puede utilizarse tanto entre ordenadores y la red de telefonía fija o móvil, siendo accesible tanto desde el Smartphone como desde un PC.

A continuación, trasladamos algunas de las cuestiones que pueden resultar más relevantes en materia de protección de datos y seguridad de la información en el uso de esta plataforma:

- Términos y privacidad de Google
- Información que recoge Google

Cisco Webex

Cisco Webex es una plataforma de colaboración en la nube que facilita a los usuarios que se comuniquen vía texto (mensajería instantánea), voz (VoIP) o vídeo desde y hacia cualquier punto del mundo. También permite

realizar llamadas entre ordenadores y la red de telefonía fija o móvil, y se puede acceder tanto desde el Smartphone como desde un PC.

Sobre la misma, el Centro Criptológico Nacional ha emitido unas recomendaciones y buenas prácticas para su uso en reuniones por los usuarios, indicando soluciones que aporta sobre aspectos prácticos en el entorno laboral como por ejemplo, prevenir el reenvío de invitaciones, habilitar a un anfitrión para administrar de forma segura una reunión de la sala personal y administrar el control de compartición de archivos.

A continuación, trasladamos las cuestiones que pueden resultar más relevantes en materia de protección de datos y seguridad de la información en el uso de esta plataforma, incluyendo las recomendaciones y buenas prácticas publicadas por el CCN-CERT:

- Declaración de privacidad
- Uso de Cisco Webex, sus implicaciones para la seguridad y privacidad. Recomendaciones y buenas prácticas.

Microsoft Teams

Microsoft Teams es una plataforma creada para hacer posible la comunicación entre los usuarios vía texto (mensajería instantánea), voz (VoIP) o vídeo en cualquier punto del mundo. Al igual que las demás, permite realizar llamadas entre ordenadores y la red de telefonía fija o móvil y se puede acceder tanto desde el Smartphone como desde un PC, forma parte del paquete 365 de Microsoft Office.
Al ser una herramienta de Microsoft permite a aquellos usuarios que dispongan de las herramientas de Mircrosoft tener acceso a notas y documentos gracias a la integración con OneNote y SharePoint y trabajar con documentos de Office Online directamente desde Teams.
A continuación, trasladamos las cuestiones que pueden resultar más relevantes en materia de protección de datos y seguridad de la información en el uso de esta plataforma, incluyendo el acceso a la guía de configuración segura para los usuarios sobre el uso de Microsoft Teams publicada por el CCN-CERT:

- Guía de configuración segura para Microsoft Teams
- Privacidad en Microsoft Teams

Zoom

Permite el intercambio entre usuarios de comunicación vía texto (mensajería instantánea), voz (VoIP) o vídeo desde cualquier lugar, se pueden realizar llamadas entre ordenadores y la red de telefonía fija o móvil, y acceder tanto desde el Smartphone como desde un PC. Al igual que ocurre con la aplicación Webex, el Centro Criptológico Nacional ha elaborado un documento que recoge recomendaciones para su uso en reuniones por los usuarios.

A continuación, trasladamos las cuestiones que pueden resultar más relevantes en materia de protección de datos y seguridad de la información en el uso de esta plataforma y algunas recomendaciones al respecto emitidas por el CCN-CERT:

- Políticas legales y de privacidad

- El uso de Zoom y sus implicaciones para la seguridad y privacidad. Recomendaciones y buenas prácticas por el Centro Criptológico Nacional, CCN-CERT

Orientaciones para el correo electrónico

En el escenario del teletrabajo en el que accedemos al sistema de correo electrónico corporativo desde equipos informáticos no gestionados por la entidad a través de internet, es recomendable reforzar la inspección de los e-mails antes de ser entregados a los usuarios. De lo contrario, las probabilidades de ser víctima de un ataque se incrementan considerablemente, dado que los ordenadores particulares, en remoto, pueden no garantizar una seguridad adecuada.

Además, es importante **controlar los motores de antivirus e inspeccionar los buzones de correo electrónico hacia atrás en el tiempo**, siempre que tengamos tanto acceso remoto como acceso al correo electrónico corporativo. Y debemos tener en cuenta que **no se deberían utilizar datos sensibles de la entidad o información que legalmente deba ser protegida**, **en equipos que no pertenezcan a la entidad**.

> ***"En el escenario del teletrabajo, en el que accedemos al sistema de correo electrónico corporativo desde equipos informáticos no gestionados por la entidad a través de internet, es recomendable reforzar la inspección de los e-mails antes de ser entregados a los usuarios. De lo contrario, las probabilidades de ser víctima de un ataque se incrementan considerablemente, dado que los ordenadores particulares, en remoto, no garantizan una seguridad adecuada"***

MATERIAL COMPLEMENTARIO

- Destacar de nuevo las Recomendaciones de la AEPD para proteger los datos personales en situaciones de movilidad y teletrabajo. Consulta este enlace. 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**"*

- Recomendaciones de Seguridad para situaciones de teletrabajo y refuerzo en vigilancia del Centro Criptológico Nacional, CCN-CERT. Consulta este enlace.

- Anteproyecto de ley de Trabajo a Distancia. Consulta este enlace

NOTICIAS

- **El Tribunal de Justicia de la Unión Europea (TJUE) ha invalidado el sistema de intercambio de datos del llamado «Privacy Shield»** («Escudo de privacidad», en español) entre la Unión Europea (UE) y los EE. UU al entender que existe una «excesiva vigilancia» por las autoridades estadounidenses. 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.

- **¿Puede tener acceso ilimitado la Policía a tus datos personales?** El Constitucional alemán restringe el acceso de la policía a los datos privados de los ciudadanos. Consulta este enlace con las implicaciones.

- **Sanción de 40.000 € (24.000 al beneficiarse de las 2 reducciones de la LEY 39/2015) a Iberia, impuesta por la Agencia Española de protección de Datos por no facilitar el derecho de acceso** a unas grabaciones. Anteriormente la AEPD había resuelto el procedimiento concediendo el acceso. Consulta este enlace con la sanción.

- **La tecnología 5G llega para quedarse** y aunque ofrece importantes mejoras a los usuarios también puede implicar ciertos riesgos para la privacidad. La Agencia ha publicado un análisis que incluye recomendaciones relacionadas con la Protección de Datos. Consulta este enlace.

- **¿Puede ser el Reconocimiento facial nuestra entrada en conciertos y otros eventos?** Futuro plan que preocupa por su falta de privacidad. Consulta este enlace. Por su parte la Agencia Española de Protección de Datos realizo una guía con recomendaciones al respecto, consulta este enlace.