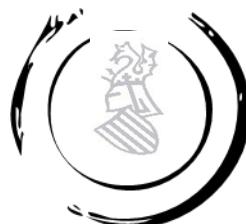




Protecció de Dades i Seguretat de la Informació



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 22 | Abril 2022

PRIVACIDAD EN REUNIONES ONLINE



Í N D I C E



PRIVACIDAD EN REUNIONES ONLINE

	Página
Introducción	2
Recomendaciones de seguridad en reuniones online	3
Sanción por grabar y difundir una reunión online	5
Noticias y material complementario	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: dpdsi@dival.es

SUSCRIPCIONES

Si deseas suscribirse a nuestro Boletín informativo accede al siguiente [enlace](#)



INTRODUCCIÓN



Las reuniones *online* se han visto potenciadas en nuestra organización con motivo de la pandemia de la Covid-19. No obstante, las sesiones y aplicaciones de videoconferencia deficientemente protegidas son un vector de ataque para los ciberdelincuentes.

Por esta razón, resulta imprescindible adoptar una serie de buenas prácticas en su utilización, con el fin de minimizar los riesgos asociados al empleo de las mismas. Tomando algunas precauciones básicas, podremos garantizar que las reuniones *online* sean un espacio de trabajo eficaz y seguro, evitando incidentes que puedan llegar a constituir una brecha de seguridad de los datos personales o comprometer de otra forma la privacidad.

En la Diputación de Valencia, conscientes del uso cada vez más acentuado de este tipo de tecnologías, damos traslado de una serie de recomendaciones que, a nivel general, permitirían mejorar la privacidad en este tipo de comunicaciones.

**“LAS SESIONES Y APLICACIONES DE VIDEOCONFERENCIA DEFICIENTEMENTE
PROTEGIDAS SON UN VECTOR DE ATAQUE PARA LOS CIBERDELINCUENTES. TOMANDO
ALGUNAS PRECAUCIONES BÁSICAS, PODREMOS GARANTIZAR QUE LAS REUNIONES
ONLINE SEAN UN ESPACIO DE TRABAJO EFICAZ Y SEGURO”.**



RECOMENDACIONES DE SEGURIDAD EN REUNIONES ONLINE



Utiliza, exclusivamente, la **aplicación del proveedor tecnológico aprobado por la organización**.



Utiliza, únicamente, **dispositivos proporcionados y/o aprobados por la organización**.



Descarga la aplicación, únicamente, de **repositorios oficiales o de la web del proveedor**.



Mantén **actualizada** la aplicación de videollamada a la **última versión disponible**.



En **reuniones con un número elevado de personas asistentes y de diversas organizaciones**, es conveniente designar, al menos, una **persona participante que ayude al organizador u organizadora durante su desarrollo en el control de estas personas y en cuestiones relativas a la privacidad y seguridad**.



Piensa por adelantado en la **sensibilidad de los temas a tratar**. Si el asunto de la reunión es sensible, bien por el tema a tratar, la identidad de las personas participantes o cualquier otra cuestión, utiliza **códigos, URLs de enlace y/o pines de acceso de un solo uso**. Además, considera la necesidad de utilizar **autenticación de doble factor**. Esto evitara que alguien pueda unirse simplemente averiguando la URL de enlace o el código de acceso.



Nunca proporciones, ni de forma oral ni por el chat, **contraseñas**.



Envía la convocatoria a **contactos concretos**, evitando el envío de convocatorias a grupos o listas de correos, que incluyan enlaces que sean válidos por su mera posesión.



Es recomendable la utilización de una '**sala de espera**' para poder ir admitiendo a las personas participantes.



No aceptes llamadas/chats de usuarios que no conozcas. Todos los usuarios deben de entrar con un **nombre/nick** reconocible para la persona que administra o modera la llamada.



Antes de iniciar la reunión, comprueba qué área es visible detrás y qué información personal está revelando. Considera la utilización de un **fondo virtual** que enmascare el segundo plano.



Si te encuentras en casa, **avisa a posibles convivientes que se va a iniciar una reunión** y toma las medidas oportunas para que su actividad no esté al alcance del micrófono y la cámara.



No grabes la reunión a menos que sea necesario. En ese caso, solicita la opinión del Delegado de Protección de Datos, que valorará la necesidad y legitimación de la grabación y, en su caso, supervisará que se informa adecuadamente a las personas asistentes de conformidad con la normativa de protección de datos.



Más allá de temas de eficiencia en la comunicación, durante la reunión, es recomendable **desactivar el micrófono y la recogida de video cuando no sea necesario**. En particular, si va a realizar alguna acción fuera del foco de la cámara. Presta especial atención a los micrófonos inalámbricos.



Si durante la llamada decides **compartir pantalla** con el resto de usuarios, **asegúrate de que no revelas información** como: nombres de usuario o de dispositivo, documentos confidenciales, nombres de archivos o directorios sensibles, etc.



Cuando termine la reunión, asegúrate de utilizar un **dispositivo que inhabilite físicamente la cámara (pestaña, adhesivo o similar)**. No retires el dispositivo hasta que se vaya a iniciar de nuevo una conexión.



SANCIÓN POR GRABAR Y DIFUNDIR UNA REUNIÓN ONLINE



1/74

- Procedimiento PS/00368/2021

- RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

Mediante Acuerdo de fecha 30/07/21, se inició el procedimiento sancionador, PS/0368/2021, instruido por la Agencia Española de Protección de Datos a la REAL FEDERACION ESPAÑOLA DE FUTBOL, (RFEF) con CIF.: Q2878017I, (en adelante, "la parte reclamada"), en virtud de las reclamaciones presentadas por la ASOCIACIÓN DE FUTBOLISTAS ESPAÑOLES (AFE) y por la LIGA NACIONAL DE FUTBOL PROFESIONAL (LNFP), (en adelante, "las partes reclamantes"), por presunta infracción del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27/04/16, 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 (RGPD) y de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, (LOPDGDD), y teniendo como base:

HECHOS

Recientemente, una entidad ha sido sancionada por la Agencia Española de Protección de Datos ([Procedimiento PS/00368/2021](#)) por grabar una reunión celebrada en la plataforma *Zoom* y, además, ceder los datos a los medios de comunicación.

La Real Federación Española de Fútbol (RFEF) grabó una reunión celebrada el 7 de abril de 2020 con otros entes de carácter deportivo para tratar la cuestión del impacto de la emergencia sanitaria en el mundo del fútbol. Posteriormente, la Federación difundió extractos de los ficheros de audio entre algunos medios de comunicación sin el conocimiento ni consentimiento de sus participantes, que lo descubrieron cuando fueron emitidos en antena.

Los reclamantes denunciaron que, en ningún momento se les informó de que iba a ser grabada, ni tampoco de los aspectos relativos al tratamiento de los datos personales contemplados en el art. 13 RGPD. Por su parte, la Federación alegó que en una reunión previa (del 12/03/20), el responsable de la RFEF dijo al comienzo de la misma: "*(...) Estamos grabando la reunión para que quede constancia de todo*".

La AEPD señala, en primer lugar, que a la segunda reunión asistieron personas que no habían asistido a la primera y que no tenían por qué tener conocimiento de que la reunión iba a ser grabada ni del contenido de la primera reunión. En segundo lugar, se constata que **los asistentes no fueron informados convenientemente de que su reunión iba a ser grabada ni de los extremos del artículo 13 del RGPD**: a) la identidad y los datos de contacto del responsable y, en su caso, de su representante; b) los datos de contacto del delegado de protección de datos, en su caso; c) de los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento; d) los destinatarios o las categorías de destinatarios de los datos personales, en su caso; e) en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional; f) el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados



para determinar este plazo; g) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos; y h) el derecho a presentar una reclamación ante una autoridad de control.

Tampoco se informó a los asistentes de que la grabación iba a ser cedida a los medios de comunicación tal y como establece el artículo 13.3 del RGPD: “*Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente a tenor del apartado 2*”.

Señala la AEPD que el artículo 18 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (LRJSP), posibilita que las reuniones de un órgano colegiado pueden ser grabadas a efectos de acompañar al acta de la sesión y darle prueba de legitimidad e integridad: “*(...) El fichero resultante de la grabación, junto con la certificación expedida por el Secretario de la autenticidad e integridad del mismo, y cuantos documentos en soporte electrónico se utilizasen como documentos de la sesión, podrán acompañar al acta de las sesiones (...)*”. De acuerdo con lo anterior, **la AEPD entiende que la RFEF sí tenía la legitimación necesaria para grabar las sesiones de la “Comisión de Seguimiento del COVID-19”**, pero únicamente para dar soporte al acta de la reunión y en este sentido se debería haber informado a los asistentes según el artículo 13 del RGPD: “*1. Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación: (...)*”, entre la que se encuentra en el punto c): “*los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento*”

Sobre la posibilidad de hacerlas públicas, manifiesta la AEPD que no se deben confundir conceptos tan diferentes como son el acta de una reunión de un órgano colegiado (definida en el artículo 18.1 de la LRJSP, párrafo 1º) con la posible grabación de la reunión y su finalidad (definida en el artículo 18.1 de la LRJSP, párrafo 2º). **El hecho de que exista el derecho de acceso al acta de una reunión de un órgano colegiado de carácter público, en base a lo estipulado en la Ley 19/2013, de Transparencia y Buen Gobierno, no implica que se pueda acceder también a la grabación de la reunión, pues no tienen el mismo contenido ni finalidad**. En las actas de las reuniones de los órganos colegiados se incluyen “los puntos principales de las deliberaciones” y no se incluye la transcripción íntegra de la intervención o propuesta o las opiniones o comentarios personales de los intervenientes, a no ser que, expresamente así lo indiquen. Por tanto, a juicio de la AEPD, no es lo mismo una grabación de la reunión de un órgano colegiado que el acta de la sesión, pues **en las grabaciones, además de constar datos personales de los asistentes, como es la voz de interveniente o su identificación con nombre y apellidos, también existe grabación de opiniones, comentarios personales o pensamientos que no tienen nada que ver con el asunto tratado en la reunión**.

“NO GRABES LA REUNIÓN A MENOS QUE SEA NECESARIO. EN ESE CASO, SOLICITA LA OPINIÓN DEL DELEGADO DE PROTECCIÓN DE DATOS, QUE VALORARÁ LA NECESIDAD Y LEGITIMACIÓN DE LA GRABACIÓN Y, EN SU CASO, SUPERVISARÁ QUE SE INFORMA ADECUADAMENTE A LAS PERSONAS ASISTENTES DE CONFORMIDAD CON LA NORMATIVA DE PROTECCIÓN DE DATOS”.



MATERIAL COMPLEMENTARIO

- Privacidad en reuniones online (AEPD). Consulta el blog en [este enlace](#).
- Aplica estos consejos y protege tus videollamadas (INCIBE). Consulta el blog en [este enlace](#).
- Videollamadas: riesgos asociados a su uso y recomendaciones de seguridad (INCIBE). Consulta el blog en [este enlace](#).
- Cómo teletrabajar de forma segura sin poner en riesgo a usuarios y organizaciones (CCN). Consulta [este enlace](#).
- Plataformas de videoconferencia y aspectos de seguridad que te interesa conocer (Oficina de Seguridad del Internauta). Consulta el blog en [este enlace](#).
- *Preventing Eavesdropping and Protecting Privacy on Virtual Meetings* (National Institute of Standards and Technology). Consulta [este enlace](#).
- Procedimiento PS/00368/2021 (AEPD). Consulta [este enlace](#).

NOTICIAS

- **La AEPD publica su Memoria de actuación 2021.** La Agencia Española de Protección de Datos publica su Memoria 2021, que recoge las actividades realizadas por este organismo en todas sus áreas, un análisis de las tendencias y una exposición de los retos presentes y futuros. Consulta la Memoria en [este enlace](#).
- **La APDCAT se pronuncia sobre la comunicación, por parte de un Ayuntamiento al INSS, de un certificado de empadronamiento histórico colectivo para gestionar el ingreso mínimo vital.** El organismo competente para gestionar el ingreso mínimo vital dispone de una vía específica de acceso a los datos del Padrón municipal que resulten necesarios para la tramitación de la prestación, que es la consulta de esta información de los padrones de la que dispone el INE (artículo 21 Ley 19/2021). En caso de no coincidencia entre los datos consultados en el INE y los especificados en la solicitud de la prestación, este organismo puede requerir al interesado la aportación del certificado de empadronamiento histórico y colectivo. En caso de no aportarlo, puede requerir esta información al Ayuntamiento en base a la habilitación que confiere el artículo 28.2 de la LPAC, salvo que alguna de las personas afectadas se oponga. En cualquier caso, es importante advertirles de las consecuencias de esta oposición. Consulta el Dictamen en [este enlace](#).
- **La AEPD aclara si en los procesos selectivos de acceso al empleo público se ha de dar publicidad al dato de la condición de discapacidad.** Entiende la AEPD que existe legitimación para publicar las listas de participantes, y en su caso, aprobados, por el turno de discapacidad en un procedimiento de concurrencia competitiva. Ahora bien, con respecto al dato de discapacidad, dado que puede provocar situaciones de discriminación, estigmatización y, en último término, riesgo de exclusión social, han de aplicarse determinadas medidas. Por ejemplo, identificándolos con un código, las iniciales de los nombres y apellidos de cada participante y el DNI en los términos de la Disposición Adicional Séptima de la LOPDGDD. Consulta el informe en [este enlace](#).