ASUNTO: PROTECCIÓN DE DATOS EN LAS VIDEO-CONFERENCIAS del PMEB.

Consulta de **RR.HH**. y de la **Coordinación Técnica de Escuelas Infantiles del Patronato** sobre la posibilidad de mantener reuniones telemáticas por videollamada con las familias a través de internet mediante software gratuito como **SKYPE, JEETSI, SKYPE** o similar. Los padres solicitan poder mantener reuniones telemáticas, ante la situación de pandemia y la limitación de acceso a los centros y de comunicación directa con las docentes. Medidas a adoptar para mantener la privacidad y la protección de datos.

El gran aumento de la prestación de servicios de forma telemática (**clases lectivas**, consultas médicas, **trámites administrativos**, **teleformación,** etc.) así como la gestión interna de las entidades (asambleas virtuales, teletrabajo, etc.), debido a la crisis originada por la Covid-19, ha obligado a las organizaciones públicas y privadas prestadoras de servicios a buscar alternativas, entre ellas, el uso de la videoconferencia para comunicarse con pacientes, alumnos/as y familiares, proveedores, afiliados/as, asociados/as, usuarios/as, clientes y otros miembros de la entidad.
En lo concerniente a **la privacidad y la protección de datos de carácter personal,** la comunicación online mediante videoconferencia, debe celebrarse en un entorno seguro que respete la privacidad de el/la interesado/a (afectado/a como titular de los datos y especialmente de su imagen), y la confidencialidad de la conversación e información suministrada, puesto que en una videoconferencia podría exponer y presentar información delicada y confidencial de los interlocutores y de las entidades, que no debe ser pública en modo alguno.

Las **medidas** a adoptar, al amparo de **la legislación vigente**[1], podrían ser las siguientes:

[1] -Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los derechos digitales (LOPD-GDD).
-Reglamento 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 (RGPD).
-Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.
-Ley Orgánica 1/1996 de 15 de enero, de Protección Jurídica del Menor. Ley 26/2015, de 28 de julio de Modificación del Sistema de Protección a la Infancia y Adolescencia.
-Ley 34/2002, de 11 de julio, de **servicios de la sociedad de la información** y de comercio electrónico

1.-MEDIDAS DE SEGURIDAD A ADOPTAR EN LAS VIDEOCONFERENCIAS.

1.1.-Con respecto a la aplicación o plataforma:

- Utilizar perfiles de usuario con autenticación mediante contraseña segura, para evitar el acceso por usuarios no autorizados.
- Mantener actualizado el software de los sistemas de videoconferencia.
- Asegurarnos, en el caso de que se utilice una aplicación o plataforma privada y no perteneciente a la Administración, que esta cumpla con todos los requisitos legales y de seguridad para que nuestras conferencias sean seguras.
- En su caso, cifrar por defecto todas las comunicaciones, utilizando el protocolo *SSL*, para establecer un canal seguro.

1.2.-Con respecto a las personas usuarias:

- Concienciar a los usuarios sobre la necesidad de aplicar estas precauciones de seguridad.
- No establecer comunicaciones con desconocidos o que no estén dentro de nuestra lista de contactos.
- Añadir únicamente a contactos conocidos de usuarios registrados dentro de nuestra lista de contactos.
- Verificar la identidad de los nuevos contactos por otros medios, sobre todo cuando vamos a iniciar una videoconferencia por primera vez con ellos.
- En ningún caso (no) proceder a grabar la videoconferencia salvo que exista un consentimiento expreso por el interlocutor para el fin exacto para el cual se procede a la grabación.
- Evitar transferencias de datos especialmente sensibles (sobre ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico y relativos a la salud) salvo que se opere por una aplicación creada y gestionada por la administración, que su transmisión haya sido solicitada por la Administración para la adecuada prestación del servicio y comprobando que se cumplen con todos las medidas de seguridad.

1.3.-<u>Con respecto al uso</u>:

- Deshabilitar la compartición de escritorio por defecto. Habilitar solo cuando sea necesario.
- Deshabilitar la recepción de video por defecto. Habilitar solo cuando sea necesario.
- Cubrir la cámara cuando el sistema no está en uso.
- Apagar o silenciar los micrófonos cuando el sistema no está en uso.

2.-<u>INFORMACIÓN A LOS INTERLOCUTORES SOBRE EL TRATAMIENTO DE DATOS PERSONALES</u>.

2.1.-Si mediante la misma **<u>no se va a recabar datos de carácter personal</u>**:

- Si es la primera vez que contactamos con el interlocutor (alumno/a, familiar, usuario/a, socio/a, cliente/a) se le debe informar de los detalles del tratamiento de sus datos personales conforme los artículos 13 y 14 del GDPR y 11 de la LOPDGDD. (Clausula informativa para sede social del documento de seguridad o <u>de política de privacidad del PMEG</u>, sin necesidad de que sea firmada por los usuarios/as).
- Si se trata de interlocutores con la que ya se tiene una relación previa a la videoconferencia (alumno/a con matriculación, familiares, cliente con contrato mercantil), no será necesario volver informar sobre el tratamiento de los datos personales siempre que la finalidad de la videoconferencia sea un medio para seguir ofreciéndole dichos servicios.

2.2.-Si mediante la misma **<u>sí se van a recabar datos de carácter personal</u>**:

- Siempre se debe informar al interlocutor de los detalles del tratamiento de sus datos personales conforme los artículos 13 y 14 del RGPD y 11 de la LOPDGDD.(Clausula informativa para sede social del documento de seguridad o <u>de política de privacidad del PMEG</u>, sin necesidad de que sea firmada por los usuarios/as).
- Se recomienda que la información anterior se facilite por capas, es decir, se aporta la información básica primero, redireccionando a otra ubicación donde se halle el resto de la información del tratamiento de los datos personales.
- Además, también es recomendable, antes de iniciar la videoconferencia que se informe al interlocutor sobre los siguientes extremos:
- La prohibición de grabar, tanto audio como vídeo, por ambas partes.

3.-LA PLATAFORMA O MEDIO POR EL CUAL TENDRÁ LUGAR LA VIDEOCONFERENCIA:

3.1.-Si **la plataforma pertenece a la Administración o a una entidad con concierto con la Administración para tal fin o a una entidad con sede en el territorio de la UE**, solo será necesario informar al interlocutor cuando sea la primera vez que se contacta con él o cuando se vayan a recabar datos personales (revisar supuestos anteriores).

3.2.-Si la plataforma pertenece a una sociedad con sede fuera del territorio de la UE, pero que **se encuentre en un país declarado adecuado por la UE** (Andorra, Argentina, Canadá, Isla de Man, Islas Feroe, Israel, Jersey, Nueva Zelanda, Suiza, Uruguay) o **se encuentre adherida al acuerdo de privacidad** (**PRIVACY SHIELD**), será necesaria la información del tratamiento de los datos de carácter personal. Se puede cotejar la adhesión de la entidad al **ACUERDO PRIVACY SHIELD** en el siguiente enlace: https://**www.privacyshield.gov/participant_search**

3.3.-Si **la plataforma pertenece a una sociedad con sede fuera del territorio de la UE y no se encuentra situada en ninguno de los supuestos anteriores**, pero **la entidad ofrece alguna otra de las garantías adecuadas**, conforme los artículos 46 a 49 del RGPD, se requerie el consentimiento expreso del interlocutor. (Comprobar garantías en la política de privacidad de la web de la entidad).

3.4.-Si **la plataforma pertenece a una sociedad que no se halle en ninguno de los supuestos anteriores**, se desaconseja realizar la videoconferencia por esos medios.

4.-CONSENTIMIENTO SOBRE EL TRATAMIENTO DE LOS DATOS PERSONALES.

4.1.-Será **necesario recabar el consentimiento del interlocutor**, en todo caso, **y con carácter previo a la videoconferencia**, en los siguientes supuestos:

- Cuando se vaya a utilizar para la videoconferencia una aplicación o plataforma de una sociedad cuya sede no se halle ubicada en la UE o no este adherida al escudo de privacidad "**PRIVACY SHIELD".**
- Si se prevé que se vaya a grabar la videoconferencia.
- Cuando se realice con menores de 14 años, se requiere en todo momento el consentimiento de los padres o tutores del menor.
- Cuando los datos que se recaben en la videoconferencia se vayan a ceder a terceros.

4.2.-No será necesario recabar el consentimiento cuando ya se haya firmado una clausula de consentimiento de tratamiento de datos personales para tal fin, por ejemplo en la matriculación del alumno/a en

un centro educativo, en la ficha de afiliación en un sindicato, o en el contrato de servicio de un cliente.

Para recabar el consentimiento del interlocutor, es recomendable utilizar la **Clausula para recabar datos** de afiliados/as, usuarios/as, clientes en el documento de seguridad o de o de política de privacidad del PMEG, debiendo ser firmada por los usuarios/as, alumnos/as, afiliados/as, clientes.

FUENTES DOCUMENTALES:

- **EL DEBER DE INFORMAR Y OTRAS MEDIDAS DE RESPONSABILIDAD PROACTIVA EN APPS PARA DISPOSITIVOS MÓVILES. Agencia Española de Protección de Datos (AEPD).** Se adjunta a este informe**.**
- **VIDEOLLAMADAS RIESGOS ASOCIADOS A SU USO Y RECOMENDACIONES DE SEGURIDAD. Instituto Nacional de Ciberseguridad (INCIBE).**
- **APLICA ESTOS CONSEJOS Y PROTEGE TUS VIDEOLLAMADAS. Instituto Nacional de Ciberseguridad (INCIBE).**[2]

[2] **El COVID-19** ha cambiado de repente, **con el TELETRABAJO**, la forma en que las empresas y organizaciones de cualquier sector se comunican. Por esa razón, **LAS APLICACIONES DE VIDEOLLAMADA** se han convertido, de un día para otro, en herramientas imprescindibles para la continuidad de la actividad diaria en esta situación tan inusual.

Este nuevo escenario no ha pasado desapercibido para **los ciberdelincuentes** que están al acecho de cualquier oportunidad. La amplia utilización de las herramientas de videoconferencia supone para ellos una forma más de hacer «caja» al aprovechar los descuidos de seguridad de las empresas y así obtener datos personales o secretos profesionales, por ejemplo para su venta o como motivo de extorsión.

Además, el aumento del uso de estas herramientas ha venido acompañado de la aparición de nuevas vulnerabilidades, algunas ya corregidas por los fabricantes, que pueden ser aprovechadas por **los ciberdelincuentes**, como la descrita en el aviso de seguridad Vulnerabilidad descubierta en el sistema de videoconferencia Zoom, y otras, como el *malware* Pykspa o ataques como Zoombombing.

Por todo ello, si vas a hacer uso de estas herramientas, sigue **ESTAS RECOMENDACIONES DE SEGURIDAD,** y revisa la política de uso de herramientas colaborativas para incluirlas.

RECOMENDACIONES DE SEGURIDAD EN EL USO DE APLICACIONES DE VIDEOLLAMADA

Las recomendaciones descritas en este artículo no están enfocadas en una herramienta específica, pero es recomendable que la aplicación elegida para realizar videollamadas nos permita elegirlas y configurarlas.

Utiliza un plan empresarial en lugar de uno básico

Mantener reuniones por videoconferencia de forma segura es imprescindible mientras esté presente el COVID-19. Debido a esta situación, **muchas empresas han decido ofrecer de forma gratuita a los usuarios sus herramientas colaborativas**, como se

muestra en **este listado elaborado por Computerworld** o las recogidas en la iniciativa Acelerapyme de Red.es.

No obstante, si utilizamos planes básicos o gratuitos de las herramientas colaborativas, no podremos aplicar algunas características de las opciones empresariales, que harán más segura su utilización. Por ello, siempre es recomendable decantarse por un **plan empresarial** verificando que cuenta con las propiedades necesarias para hacer un uso seguro.

¡QUÉ NO SE CUELE NADIE! ACTIVA LA SALA DE ESPERA Y BLOQUEA LA REUNIÓN

Esta funcionalidad **añade a los participantes de una conferencia en un entorno previo a la reunión**, así el administrador de la sala puede comprobar si los asistentes son los permitidos. Desde esta sala de espera, verificando la identidad de cada participante invitado, les dará paso a la reunión. De este modo, ante la entrada de alguien no autorizado, el administrador podrá **denegarle el acceso** a la reunión.

Una vez que todos los participantes se hayan incorporado a la llamada, se **bloqueará el acceso** a nuevos participantes a la reunión. De esta forma, aseguramos que sólo los participantes autorizados estén en la reunión evitando intrusos que puedan espiar nuestras conversaciones.

REQUERIR CONTRASEÑA PARA ACCEDER A LA REUNIÓN

El acceso a cualquier videollamada siempre debe estar protegido por medio de una contraseña lo más robusta posible. Esta es la única forma, en muchos casos, de evitar que terceros no autorizados consigan acceso.

Muchas **aplicaciones de videollamada** cuentan con esta configuración habilitada por defecto. Si la aplicación que usas no lo hace por defecto, verifícalo para forzar su uso.

¡VIGILA A QUIÉN LE PASAS LA CONVOCATORIA!

Compartir el enlace entre los participantes de una videollamada es necesario para que esta se pueda producir. Para ello, es recomendable **utilizar las funciones de compartición de las propias aplicaciones de videollamada**. Evita en todo caso el uso de redes sociales o canales de comunicación inseguros para lanzar la convocatoria.

Video y micrófono apagados por defecto y ¡cuidado con lo que compartes!

Algunas funciones por defecto, como la cámara activada o el micrófono, pueden ser motivo de situaciones poco deseables. Los participantes que se unan a una videollamada **no deben compartir su escritorio de forma predeterminada ya que esto puede provocar fugas de información**. Los usuarios de una reunión siempre accederán sin mostrar su escritorio. El administrador será quien permita que ciertos usuarios muestren su escritorio cuando sea preciso.

La **recepción de video permanecerá deshabilitada por defecto** y solo se permitirá su uso cuando sea necesario, de esta forma se evitan posibles fugas de información y se reduce el consumo de ancho de banda. El **micrófono también permanecerá apagado cuando no sea necesario su uso**.

No está de más recordar que cuando un usuario comparte su pantalla con el resto de usuarios de la reunión debe evitar compartir información confidencial, como:

- nombres de usuario o nombre de dispositivo,
- documentos confidenciales,
- nombres de archivos o directorios sensibles,
- direcciones web del navegador.

- **PRECAUCIONES PARA REALIZAR UNA VIDEOCONFERENCIA. Instituto Nacional de Ciberseguridad (INCIBE)** del Ministerio de Asuntos Económicos y Transformación Digital.[3]

Si el administrador pretende grabar la reunión, se lo comunicará a los participantes para que estos sean conscientes de ello.

***SOFTWARE* ACTUALIZADO Y DESCARGADO DESDE LA WEB OFICIAL**

La herramienta utilizada para realizar las videollamadas **siempre estará actualizada a la última versión disponible**. En caso de ser posible se marcará la opción de **actualizaciones automáticas** o que la aplicación avise al usuario en caso de existir una nueva actualización.

La herramienta debe descargarse siempre desde la web oficial del desarrollador o desde repositorios oficiales, como Google Play o App Store de Apple. Nunca se descargará de enlaces obtenidos en medios de comunicación, como el correo electrónico, aplicaciones de mensajería instantánea o redes sociales, ya que puede dirigir al usuario a sitios web fraudulentos. Con el auge de la necesidad de videollamadas, han aparecido cientos de sitios falsos en los que en lugar de descargar la aplicación descargas malware.

CONOCER LA POLÍTICA DE PRIVACIDAD DE LA HERRAMIENTA

Antes de decantarse por una herramienta de videoconferencia u otra, se debe **conocer la política de privacidad que sigue el proveedor**, así se conocerá qué tratamiento realiza sobre la información confidencial. Algunas herramientas pueden seguir políticas cuya protección para los clientes no es tan robusta como la que ofrece el RGPD, por lo que siempre hay que saber cómo actúan sobre los datos tratados.

Cifrado de las comunicaciones

Esta será una de las medidas de seguridad imprescindibles con las que contará la aplicación de seguridad, de esta forma **las comunicaciones no podrán ser espiadas por un tercero**. Generalmente **todas las principales aplicaciones cuentan con mecanismos de cifrado** pero es conveniente comprobarlo antes de decantarse por una.

La información que se envía por medio de la herramienta, como son **documentos confidenciales, se enviará cifrada previamente**, así se añadirá una capa extra de seguridad en caso de acceso no autorizado.

Siguiendo estas recomendaciones, podrás realizar videollamadas de manera segura, tanto entre tus empleados como con clientes o proveedores. Si eres un usuario de este tipo de herramientas, aplícalas y difúndelas. Vamos a intentar crear entre todos un entorno de trabajo lo más seguro posible.

Si tienes dudas, llama al **017**, la **LINEA DE AYUDA EN CIBERSEGURIDAD** de **INCIBE.** Expertos en la materia resolverán cualquier conflicto online relacionado con el uso de la tecnología y los dispositivos conectados.

[3] **¿Realizas videoconferencias de trabajo? ¿Utilizas las videoconferencias para comunicarte con tus clientes, proveedores y compañeros de trabajo? ¿Conoces algunas de las medidas de seguridad a tener en cuenta ante una videoconferencia?**

El mercado ofrece multitud de herramientas y plataformas que ofrecen servicios de videoconferencias a la medida de las necesidades de las empresas. Pueden ser gratuitas o de pago, pueden permitir compartir documentos de trabajo, disponer de

servicios añadidos como herramientas de chat o pizarras virtuales, y se pueden realizar presentaciones de la misma forma que si estuviésemos en una sala de exposiciones.

Entre los tipos de videoconferencia que podemos optar tenemos, por un lado, las **videoconferencias tradicionales**, tanto las que utilizan equipos físicos específicos dedicados a ello, como los que utilizan software instalado en ordenadores personales.

También tenemos las **videoconferencias como servicio móvil en la nube o VAAS,** donde podemos contratar el servicio sin necesidad de mantener ni instalar la infraestructura clásica de videoconferencia, conectándonos a los servidores del proveedor que está en la nube. En este sentido, podemos utilizar la versión para empresas de las principales opciones que utilizamos para nuestras comunicaciones privadas que ofrecen las funcionalidades y la seguridad que necesitan la mayoría de las pequeñas empresas.

En todas ellas hay que extremar la seguridad para prevenir la intrusión y garantizar la **confidencialidad** de las conversaciones y de la información que tratamos en ellas.

En una videoconferencia, se puede exponer y presentar información delicada y confidencial de nuestras empresas, como información de clientes y proveedores, información de productos, datos económicos, novedades o innovaciones de productos, etc. Tanto el contenido de las conferencias como las grabaciones de las mismas o la información de apoyo utilizada (presentaciones, PDF, videos, etc.) podrían estar expuestas a **las siguientes AMENAZAS:**

- Aquellas que son inherentes a las redes inalámbricas e internet.
- Aquellas que tienen como causa una configuración descuidada o errónea de las sesiones de videoconferencia.
- Aquellas que están asociadas a las carencias de seguridad de las propias herramientas o servicios de videoconferencia. Hay que verificar que los productos o servicios utilizados incluyan **funcionalidades para el cifrado de datos**, así como **funciones antimalware**.

Para garantizar **una seguridad mínima en estas comunicaciones**, debemos conocer y establecer unas **PAUTAS GENERALES DE SEGURIDAD** como las siguientes:

1. No establecer comunicaciones con desconocidos o que no estén dentro de nuestra **lista de contactos**.
2. Añadir únicamente a **contactos** conocidos y **de confianza** dentro de nuestra lista de contactos. Verificar la identidad de los nuevos contactos por otros medios, sobre todo cuando vamos a iniciar una videoconferencia por primera vez con ellos.
3. Utilizar perfiles de usuario con autenticación mediante **contraseña segura**, para evitar el acceso por usuarios no autorizados.
4. Mantener **actualizado** el software de los sistemas de videoconferencia.
5. **Deshabilitar**la compartición de **escritorio por defecto**. Habilitar solo cuando sea necesario.
6. **Deshabilitar**la recepción de **video por defecto**. Habilitar solo cuando sea necesario.
7. Cubrir la **cámara** cuando el sistema no está en uso. También, configuraremos la cámara para que, al comenzar una videoconferencia, muestre una imagen neutra que no muestre información comprometida, en caso de establecer una conexión errónea.
8. Apagar o silenciar los **micrófonos** cuando el sistema no está en uso.

- Se acompaña infografía del **INCIBE** sobre **MEDIDAS DE SEGURIDAD Y PRIVACIDAD EN PLATAFORMAS DE VIDEOCONFERENCIAS.**

Zaragoza a 1 de abril de 2021.

El **Delegado de Protección de Datos** (**DPD**). Fernando Tirado.

---

9. **Concienciar y formar a los usuarios** sobre la necesidad de aplicar estas precauciones de seguridad.

Otras **dos medidas de seguridad** que deberemos adoptar son:

1. **Cifrar** por defecto todas las comunicaciones, utilizando el protocolo *SSL*, para establecer un canal seguro. Se debe realizar siempre, aunque hay que ser especialmente precavidos cuando se estén utilizando redes cuya seguridad desconocemos.
2. Si tenemos contratado el servicio con un **proveedor externo**, asegurarnos que este cumpla con todos los requisitos legales y de seguridad para que nuestras conferencias sean seguras.

Tomando estas medidas de seguridad, podemos asegurar unas videoconferencias con nuestros socios y alumnos, familias, clientes o proveedores que resulten seguras y sin sobresaltos. **Protegiendo la confidencialidad** de la comunicación y de la información que transmitimos, **protegemos nuestra organización**.