# 20210310, Nota Informativa, privacidad en reuniones online.

En virtud de mis compromisos contractuales, seguidamente paso a comentar una publicación de la Agencia Española de Protección de Datos sobre la cuestión de la privacidad en las reuniones online.

Las reuniones virtuales online mediante voz, vídeo o a través de servicios web son una constante del trabajo actual y del teletrabajo, que se ha visto enormemente potenciado por motivo de la pandemia de la COVID-19. Si bien cada vez somos más conscientes de la necesidad de proteger nuestra privacidad y seguridad en el mundo online, con las reuniones virtuales debemos adoptar medidas específicas.

Descuidar la organización de reuniones virtuales, y prepararlas sin tener en cuenta los riesgos de privacidad, puede facilitar la práctica de conductas desleales por parte de los interlocutores, antiguos compañeros de trabajo, empleados descontentos o, incluso, que ciberdelincuentes puedan espiarlas o sabotearlas. Simplemente tomando algunas precauciones básicas se puede 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.

A continuación, se incluyen una serie de consejos básicos para mantener reuniones online con privacidad y seguridad:

- Observe y siga las políticas establecidas por su organización para las reuniones online. Esto incluye la utilización exclusiva del proveedor tecnológico aprobado por la organización.

- En reuniones con un número elevado de asistentes y de diversas organizaciones, es conveniente designar al menos un participante que ayude al organizador durante su desarrollo en el control de los asistentes y cuestiones relativas a la privacidad y seguridad.
- Piense por adelantado en la sensibilidad de los temas a tratar, la identidad de los participantes y la posible difusión en caso de que la reunión sea grabada.
- Limite la reutilización de los códigos/enlaces de acceso. Si se ha usado el mismo código/enlace durante un tiempo, probablemente lo haya compartido con más personas de las que pueda imaginar o recordar.
- Si el asunto de la reunión es sensible, bien por el tema a tratar, la identidad de los participantes o cualquier otra cuestión, utilice códigos, urls de enlace y/o pines de acceso de un solo uso. Además, considere la necesidad de utilizar autenticación de doble factor. Esto evitará que alguien pueda unirse simplemente averiguando la URL de enlace o el código de acceso.
- Deshabilite las funcionalidades no necesarias como, por ejemplo, el chat, el intercambio de ficheros o la compartición de pantalla.
- En su caso, limite quién puede compartir pantalla para evitar cualquier imagen no deseada o inesperada. Antes de que alguien comparta su pantalla, recuérdele el riesgo de compartir información sensible.

- Wealice la convocatoria únicamente a contactos concretos, evitando el envío de convocatorias a grupos o listas de correos, que incluyan enlaces que sean válidos tan solo por su posesión.
- Utilice una ‘sala de espera’ para poder ir admitiendo a los participantes, y no permita que la reunión comience hasta que se una el anfitrión.
- Habilite la notificación para cuando los asistentes se unen a la reunión. Podría ser mediante un tono característico o anunciando su nombre. Si su proveedor no lo permite, asegúrese de que el anfitrión pide a los nuevos asistentes que se identifiquen.
- Si está disponible, use un panel para comprobar los asistentes e identificar aquellos que sean genéricos.
- No grabe la reunión a menos que sea necesario. En tal caso, informe adecuadamente a los asistentes de la finalidad de la grabación y en qué momento se inicia/detiene la grabación. Algunos proveedores realizan estos avisos de forma automática.
- Antes de iniciar la reunión, compruebe qué área es visible detrás de usted y qué información personal está revelando. Considere la utilización de un fondo virtual que enmascare el segundo plano.
- Avise a posibles convivientes que se va a iniciar una reunión y tome las medidas para que su actividad no esté al alcance del micrófono y la cámara.
- Más allá de temas de eficiencia en la comunicación, durante la reunión desactive 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. Preste especial atención a los micrófonos inalámbricos

- Sea consciente de que la captura de video y audio podría continuar, por algún tipo de error humano o de sistema, cuando usted cree que la reunión ha terminado.
- Cuando termine la reunión, asegúrese de utilizar un dispositivo que inhabilite físicamente la cámara (pestaña, adhesivo o similar). No retire el dispositivo hasta que se vaya a iniciar la conexión.

La lista presentada no tiene un carácter exhaustivo, sino que se trata de una serie de consejos básicos que se deben tener en cuenta y aplicarse cuando proceda. Como conclusión general, es necesario recordar que obligatoriamente se deben conocer y cumplir las políticas de su organización, tener en cuenta la logística de la reunión y elegir las medidas apropiadas para cada situación.

En aquellos casos en los que se vayan a tratar datos o información muy sensible, es conveniente consultar con un profesional de seguridad y TI de su organización y, en su caso, tomar precauciones adicionales:

- Utilice únicamente servicios de reuniones virtuales aprobados por su organización para esas situaciones, con cifrado de extremo a extremo y que utilicen pin o contraseñas únicas para cada asistente. Dé instrucciones para que no sean compartidas.
- Utilice los paneles de asistentes para tener controlado quién está en la reunión en todo momento.

- Bloquee el acceso a la reunión una vez que todos los participantes estén identificados.
- Permita únicamente a los anfitriones compartir pantalla.
- En caso de realizar grabaciones, deben ser cifradas mediante un algoritmo robusto y utilizando contraseñas fuertes. Elimine cualquier grabación que haya podido quedar almacenada en el proveedor.
- Solicite explícitamente a los asistentes que únicamente utilicen dispositivos proporcionados y/o aprobados por la organización.

En todo caso, y como siempre, quedo a vuestra disposición para aclarar cualquier duda sobre la cuestión comentada.

Hecho conforme a mi leal saber y entender, en Manilva a 10 de marzo de 2021,


ZOTANO SANCHEZ SALVADOR - 32028277H

Firmado digitalmente por ZOTANO SANCHEZ SALVADOR - 32028277H
Fecha: 2021.03.10 00:59:01 +01'00'

**Salvador Zotano Sánchez**

**(Delegado de Protección de Datos Certificado 19-ADK0101 conforme al Esquema AEPD-DPD)**