CIBERSEGURIDADE NAS VIDEOCONFERENCIAS

RECOMENDACIÓNS XERAIS

Empregue as **ferramentas de videoconferencia corporativas** e postas a disposición pola Xunta de Galicia para o traballo remoto, evitando utilizar plataformas alleas á organización que poderían implicar riscos de seguridade (tanto técnicos como normativos).

Manteña actualizadas as aplicacións de videoconferencia que empregue, de forma que sempre teña instaladas as últimas revisións de seguridade.

Descargue as aplicacións para videoconferencias **desde as páxinas web ou tendas de aplicacións oficiais,** acudindo, sempre que sexa posible, ás indicadas pola Xunta de Galicia.

Na medida do posible, **evite facer clic nas ligazóns** que se compartan mediante o chat da sesión **se non coñece á persoa que as compartiu.**

Na medida do posible, **non comparta información persoal ou datos sensibles** (como contrasinais) durante as videoconferencias.

Como regra xeral, **non acepte chamadas ou chats de persoas usuarias que non coñeza** ou que non se atopen na súa lista de contactos. Todas deben entrar cun nome recoñecible para a persoa que modere a videoconferencia.

Cubra sempre a cámara do seu dispositivo cando non estea en uso.

Manteña pechada a aplicación de videoconferencias cando non a estea utilizando.

Deshabilite a recepción de vídeo, o micrófono e a opción de compartir escritorio por defecto. Habilite estas opcións unicamente cando sexan necesarias para garantir así que non comparte contido ou información persoal por erro.

RECOMENDACIÓNS PARA AS PERSOAS QUE CONVOCAN AS REUNIÓNS

Se vostede vai convocar unha reunión por videoconferencia siga estes consellos para asegurar a súa protección e a das persoas que van participar nela:

Use un **contrasinal seguro asociado ao seu identificador de usuario/a persoal de acceso á plataforma de videoconferencia.** Recorde que os contrasinais seguros teñen:

- Unha lonxitude mínima de 8 caracteres
- Combinan letras maiúsculas e minúsculas, números e caracteres especiais
- Non deben empregarse para varias aplicacións
- E nunca conteñen información persoal

A persoa moderadora da reunión debe **poder xestionar a conexión das persoas participantes:** pechar micrófonos, deshabilitar contidos ou sinais de vídeo. Os/as participantes non deberían ter a opción de acceder ata que non se conecte a persoa moderadora.

Teña **precaución á hora de engadir á videoconferencia a persoas que non coñeza** e verifique sempre a identidade de novos participantes, sobre todo cando é a primeira vez que vai ter unha comunicación con eles/elas.

Configure a sesión para que lle **esixa unha contrasinal de acceso ás persoas que se conecten.**

Configure a súa sesión para que **o indicador visual ou sonoro avise da entrada ou saída de persoas usuarias e desactive a resposta automática de chamadas entrantes.** Non esqueza pechar a sesión na aplicación se sabe que non vai recibir máis chamadas.

A persoa que modere a videochamada debe **xestionar se esta pode ser gravada ou non.** No caso de que se necesite gravar, a persoa que convoca **deberá informar previamente a todas as persoas participantes.** O proceso de gravación será visible durante toda a videoconferencia e para todas as persoas participantes.

A persoa moderadora debe **programar as videoconferencias co número exacto de persoas participantes.** Una vez que todas entren na sesión, debe **pechar o acceso** a novos/as participantes.

Problemas? dúbidas?

Recorde que en caso de dúbidas, se detectou un acceso non autorizado durante unha videoconferencia ou calquera outro problema de seguridade, pode poñerse en contacto co seu **Centro de Atención ao Usuario (CAU) de referencia (aquel co que contacte habitualmente).**

galicia
amtega Axencia para a Modernización Tecnolóxica
XUNTA DE GALICIA