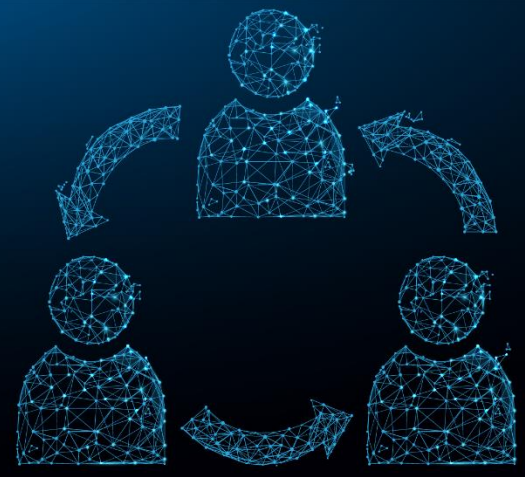
centro criptológico nacional



#CiberCOVID19

Cybersecurity recommendations for video calls and virtual meetings.

Only download applications from official marketers, such as Google Play or Apple Store, or from the supplier's website (Microsoft, Google, Cisco, etc.).

The moderator of the meeting must be able to manage the connection of the participants, close microphones, disable content or video signal. The participants should not access the meeting until the moderator connects.

Keep the video calling applications you use updated.

Consider video calls an insecure communication channel, don't give out sensitive data like passwords.

As far as possible, avoid clicking on links that are shared in the session chat, especially if you do not know the person who has shared it.

Set the session so that a visual or audible indicator warns of incoming or outgoing users and disable the automatic answer to incoming calls. Log out of the application if you know no one is going to call.

Schedule video calls with the exact number of participants. When all users have entered the session, close the access to new participants.

Do not accept calls/chats from users you do not know. In private conferences all users must enter with a recognizable name/nick-name for the administrator/moderator of the call.

All users must access to the meeting with a password. In public applications, sign up with passwords that you haven´t used on other services and do not publicly share the meeting ID.

The moderator of the video call can manage if the call can be recorded. If it is being recorded, a visual and sound indicator must be shown to all the users.

centro criptológico nacional