The following requirements, regardless of the technology used in the SCHOOL/CUSTOMER, are necessary for the correct functioning of IMTLazarus:

- It is required that the Wi-Fi infrastructure at the center works properly and without micro-cuts.
- If there is a network firewall, allow two-way communication in TCP, UDP and Secure WebSockets (WSS) with the addresses of **manager.imtlazarus.com** (**manager-usa1.imtlazarus.com** in USA) and **[school_server].imtlazarus.com**
- The ports used are:
    - 443 and 80
    - 9001-9004 TCP (9001-9002-9003-9004) " websocket port"
    - 8991-8994 TCP (8991-8992-8993-8994) " websocket port"
    - 8999 TCP

Technical specifications for Chromebook/Google Workspace devices:

- The IMTLazarus Deployment Manager must have administrator access to Google Workspace in order to install the IMTLazarus extension.
- The IMTLazarus extension will be loaded only on the Organizational Units / Licensed Groups. (See document in imtlazarus.com/en → Resources → Administrators → Installation guides and use → GOOGLE WORKSPACE EXTENSION INSTALLATION).
- To have a Google Workspace educational license managed by the school center.

We recommend:

- Having a link to the Google Workspace properly activated for an import of data. (See document in imtlazarus.com/en → Resources → Administrators → Installation guides and use → IMPORT DATA FROM GOOGLE WORKSPACE)

Technical specifications for Android/Samsung devices:

- The device version has to be Android 8.0 or higher (improved security on Samsung devices with Knox technology).
- The required data is email.
- The only browser application allowed will be IMTGo.

Technical specifications for Windows/Intune devices:

- The device version has to be Windows 10 or above.
- The required data is: the device serial number or the Azure user always with the MDM Intune.
- The only browsers allowed will be: Google Chrome and MS Edge Chromium (other browsers or portable versions will be blocked)
- The only antivirus used has to be Windows Defender.

We recommend:

- That the account used by the student must be limited, without system administrator permissions.
- That the student does not know the administrator account password.

Technical specifications for iOS devices:

- The device version must be iOS 15 or above.
- The only browser application allowed to ensure security will be IMTGo.
- The required data are: the email and the serial number for automatic deployment using MDM.

We recommend:

- That the devices are monitored with the aim of managing navigation in other browsers and controlling the profiles that manage the different applications.
- That when devices are NOT monitored (BYOD devices) we should rely on the system "Time of Use" in order to limit the use of unauthorized applications.
- That they are linked to the MDM through DEP.