Technical requirements

The following requirements, regardless of the technology used in the CLIENT/COLLEGE, are necessary for the proper functioning of IMTLAZARUS:

- It is necessary that the Wifi infrastructure of the centre works properly and without micro cuts.
- Access through at least the ports: 53 UDP, 9999 UDP and 443 TCP and allow WebSocketSecures - WSS protocol on TCP port 8999 to the assigned server address (https://[id_school_server].imtlazarus.com).
- That there is no firewall that severs the connection to the server IP. If positive, an exception rule should be added.

Technical specifications for Chromebook/Google Workspace devices:

- A properly activated link to Google Workspace is required.
- Extension of IMTLAZARUS loaded only in organizational units/ licensed groups.

Technical specifications for Android/Samsung devices:

- The device version has to be Android 6.0 or higher (complete security only on Samsung devices with Knox technology).
- The required data are: the email and the serial number of the corresponding device.

Technical specifications for Windows/Intune devices:

- The device version has to be Windows 8 or higher (complete security only on Samsung devices with Knox technology).
- The necessary data is: the email and that the serial number of the device exactly matches the actual used, otherwise it would not be possible to deploy the system through Intune.
- Devices cannot have system administrator permissions.
- You can only have Windows Antivirus, no other.
- Installed browsers need to be only: Google Chrome and MS Edge Chromium.

Technical specifications for IOS devices:

- The device version has to be IOS 10 or higher.
- Devices must be monitored (optionally, within DEP).
- The required data are: the email and the serial number of the device exactly match the one registered in the MDM for proper recognition in the security application.