Requisitos técnicos (V300725)

Los siguientes requisitos, independientemente de la tecnología utilizada en el CLIENTE/COLEGIO, son necesarios para el correcto funcionamiento de IMTLazarus:

- Se precisa que la infraestructura WiFi del centro funcione correctamente y sin microcortes.

- Si hay firewall de red, que se permita la comunicación bidireccional en TCP, UDP y WebSockets Seguros (WSS) con las direcciones de **manager.imtlazarus.com** (**manager-usa1.imtlazarus.com** en USA) y [**servidor_colegio].imtlazarus.com**.

- Los puertos utilizados son:
    - 443 y 80
    - 9001-9004 TCP (9001-9002-9003-9004) "puerto websocket"
    - 8991-8994 TCP (8991-8992-8993-8994) "puerto websocket"
    - 8999 TCP

- Habilitar la regla de firewall para el protocolo ICMP (Internet Control Message Protocol) -> concretamente permitir **ping** a la IP **8.8.8.8**

Especificaciones técnicas para dispositivos Chromebook/Google Workspace:

- Es necesario que el responsable del despliegue de IMTLazarus tenga acceso como administrador a Google Workspace para poder instalar la extensión de IMTLazarus.

- La extensión de IMTLazarus se cargará únicamente en las unidades organizativas / grupos con licencia. (Ver documento en imtlazarus.com → Recursos → Administradores → Guías de instalación y uso → CARGA EXTENSIÓN GOOGLE WORKSPACE)

- Poseer una licencia educativa de Google Workspace gestionada por el centro.

Recomendamos:

- Tener un enlace al Google Workspace correctamente activado para una importación de datos. (Ver documento en imtlazarus.com → Recursos → Administradores → Guías de instalación y uso → IMPORTACIÓN DE DATOS DESDE GOOGLE WORKSPACE)

Especificaciones técnicas para dispositivos Android/Samsung:

- La versión de los dispositivos tiene que ser Android 8.0 o superior (seguridad mejorada en dispositivos Samsung con tecnología Knox).

● El dato obligatorio necesario es el email.

● La única aplicación de navegador permitida será IMTGo.

Especificaciones técnicas para dispositivos Windows/Intune:

● La versión de los dispositivos tiene que ser Windows 10 o superior.

● Los datos necesarios son: el número de serie del dispositivo o el usuario Azure siempre con el MDM Intune.

● Los únicos navegadores permitidos serán: Google Chrome y MS Edge Chromium (el resto de navegadores o versiones portables estarán bloqueados)

● El único antivirus utilizado ha de ser Windows Defender.

Recomendamos:

● La cuenta utilizada por el estudiante deberá ser limitada, sin permisos de administrador del sistema.

● Que el estudiante no conozca la contraseña de la cuenta de administrador.

Especificaciones técnicas para dispositivos iOS:

● La versión de los dispositivos tiene que ser iOS 15 o superior.

● La única aplicación de navegador permitida para garantizar la seguridad será IMTGo.

● Los datos obligatorios necesarios son: el email y el número de serie para un despliegue automático mediante MDM.

Recomendamos:

● Que los dispositivos estén supervisados con el objetivo de administrar la navegación en otros navegadores y controlar los perfiles que gestionan las diferentes aplicaciones.

● Que cuando los dispositivos NO estén supervisados (dispositivos BYOD) debemos apoyarnos en el sistema "Tiempo de Uso" con el objetivo de limitar la utilización de aplicaciones no permitidas.

● Que estén vinculados al MDM a través de DEP.