

PREGUNTAS Y RESPUESTAS IMTLAZARUS

Este documento pretende dar respuesta a las preguntas más consultadas desde los diferentes perfiles involucrados en la comunidad educativa.

- **Preguntas 1 - 16, van dirigidas al Informático o Coordinador TIC de un centro educativo.**
- **Preguntas 17 - 24, dirigidas al profesor/a y equipo directivo del colegio.**
- **Preguntas 25 - 32, preguntas que interesan especialmente a las familias de los menores.**
- **Preguntas 33 - 34, preguntas para el distribuidor.**

1- ¿Por qué el nombre de IMTLazarus y en qué se basa?

"IMT" significa Integrated Modular Technology. Se basa en relacionar tecnología de conectividad y software de red. "Lazarus" recoge esta experiencia y lo orienta a la movilidad.

2- En el colegio ya tenemos un MDM para iPads, ¿es lo mismo que IMTLazarus?

Actualmente IMTLazarus tiene las funciones propias de un MDM para iPads por lo que no sería necesario disponer de ambas soluciones, si bien, nuestra filosofía es integrarnos con la tecnología que tenga el centro, nos complementamos.

3- ¿Con qué MDMs se integra IMTLazarus?

Actualmente con Cisco Meraki, Airwatch, Jamf School (antiguo Zuludesk), Gsuite, Samsung Knox, Microsoft Intune.

4- Entonces, ¿IMTLazarus supone una alternativa o es un complemento a los sistemas MDM actuales?

Ambas cosas, si el colegio desea continuar con su actual MDM seremos el complemento perfecto. Si prefiere quedarse únicamente con IMTLazarus disponemos de nuestro propio MDM. Podríamos decir que un MDM está dirigido hacia la seguridad del dispositivo, en cambio IMTLazarus se dirige hacia las personas, es decir, permite de un modo sencillo e intuitivo la supervisión del dispositivo por parte del profesorado o de la familia. bajo la misma herramienta para evitar conflictos de uso/configuración y siempre en función del derecho de acceso en base al horario lectivo.

5- Los dispositivos ya están enrolados en un MDM y deben permanecer en él, ¿es posible la convivencia con vuestra solución?

La convivencia es perfectamente posible con el MDM que dispongas, tal como se indica en el punto anterior.

6- ¿Cómo lográis comunicaros con MDMs u otros dispositivos de seguridad y conectividad?

Si está disponible, nos comunicamos mediante la API oficial que ofrecen. En el caso de que la información que ofrece o que simplemente no se proporcione un API, empleamos técnicas que simulan la gestión manual por parte de un administrador.

7- ¿Qué dispositivos (tablets, portátiles) podría usar para IMTLazarus?

IMTLazarus es una herramienta desarrollada para las principales tecnologías que actualmente tenemos en el mercado: iPad, Android (principalmente Samsung), Windows, Chromebook y Mac.

8- ¿Qué acciones permite la integración de un MDM con IMTLazarus?

IMTLazarus se comunica con el MDM facilitando a los distintos supervisores (profesores, familia, responsables de departamentos) la realización de acciones a través de una interfaz personalizada en tiempo real sin la necesidad de un administrador. Estas acciones serán las que se trasladen al MDM, por ejemplo el control de cámara, bloqueo/permiso de aplicaciones, control sobre YouTube, etc.

9- La implantación sería para determinados usuarios del MDM, no para todos. ¿Es posible individualizar el pago de la licencia para estos usuarios?

Por supuesto. Puedes elegir el número de usuarios que desees y pagar sólo por ellos, aunque estén registrados en diferentes cuentas de MDM. o incluso en MDM diferentes en función del dispositivo/tecnología.

10- Respecto al control de acceso, ¿cuál es la diferencia entre cómo actúa un MDM e IMTLazarus?

El MDM actúa a nivel de aplicación, te restringe el uso o no de iniciar un programa. En el navegador web todo esto se hace más complejo, no se trata de bloquear o permitir el uso de un navegador, porque el navegador hay que usarlo prácticamente casi siempre ya que es el que nos proporciona acceso al contenido de Internet y no se puede estar agregando direcciones web de bloqueo al navegador, sería poco práctico de gestionar en el tiempo. Debe actuarse en la capa de conectividad a través de un sistema basado en categorías, es decir como actúan los sistemas perimetrales de seguridad. La importancia del servicio IMTLazarus es que lleva esa seguridad a cualquier dispositivo, independientemente de donde se halle.

11- ¿Esto no va a producir lentitud en todos mis dispositivos?,¿qué ocurre si el servicio de control se cae?

La velocidad del dispositivo es la que le proporcione la conectividad que disponga. A diferencia de otros métodos basados en proxys http/https aquí no se producirán cuellos de botella lo que conduciría a una lenta navegación. El sistema basa el control sobre toda la actividad DNS que realice el dispositivo. Ante una posible caída temporal del servicio IMTLazarus, los dispositivos consultarían su configuración interna con lo cual proseguirían sin pérdida de conectividad, aunque brevemente sin los controles de acceso web.

12- ¿Hay diferencias importantes en seguridad según el dispositivo elegido?

No, no hay diferencias importantes. Todos los dispositivos ofrecen la misma protección respecto a los contenidos web y a la gestión del uso de los mismos. Con respecto al uso de aplicaciones en cada dispositivo, la seguridad es muy parecida, y se aplica de acuerdo con la tecnología empleada mediante el control de aplicaciones, apps y extensiones.

13- ¿Es necesario que implemente algo en mi infraestructura de red?

No es necesario. Es un servicio que funciona en la nube. Si bien hay ciertos requisitos importantes a considerar:

- Necesitamos que la infraestructura Wifi del centro funcione correctamente y sin microcortes.
- Acceso a través de los puertos: 9999 UDP, 53 UDP y TCP 443.
- Que no exista un firewall que corte la conexión con la IP del servidor, de ser así habría que añadir regla de excepción, ni bloquee la posible conexión VPN para iOS y Android.

14- ¿Cuál sería el motivo de tener que instalar el OpenVPN para IMTLazarus?

Mediante OpenVPN controlaremos toda la conectividad del dispositivo. En las tablets es necesario instalar estas app para establecer la comunicación de control con el servidor:

OpenVPN Connect (en la tecnología IOS) y OpenVPN for IMTLazarus en Android.

15- Quiero estudiar la solución, ¿puedo probarla en mis dispositivos?

Si, puede probar a través de un piloto de 30 días de servicio activo. Se desplegaría para el número y tipo de dispositivos que se considere. Esta gestión se tramitará a través de su distribuidor de confianza. Previamente todos los datos necesarios deben ser facilitados antes de la activación.

16- Buscamos manejar todo lo que se pueda mediante el MDM, pero no me queda claro el motivo por el que necesitan tener acceso total al MDM. Tengan en cuenta que tenemos un servicio que está en marcha.

Enlazaremos la plataforma contra su MDM (debemos saber si es por ejemplo Cisco Meraki, Airwatch o Jamf School). No modificaremos absolutamente nada de su configuración actual. Lo que conseguimos es que el profesor realice acciones inmediatas contra las cámaras, aplicaciones, etc.. sin depender del administrador. Para esa relación es necesario registrar una cuenta de administrador (la que esté en uso o generar una nueva).

17- ¿Cuáles son las funcionalidades más relevantes en IMTLazarus?

Consulte los siguientes enlaces en la sección de contenidos de la web www.imtlazarus.com:

<http://www.imtlazarus.com/wp-content/uploads/2019/12/IMTLazarus-comparativa-MDM-iOS-.pdf>

<http://www.imtlazarus.com/wp-content/uploads/2020/01/Integraci%C3%B3n-Intune-IMTLazarus.pdf>

18- Como director de un colegio, me preocupa el aspecto legal, ¿hasta qué punto se controla el dispositivo?

IMTLazarus controla los accesos a las aplicaciones y a las webs. No está permitido legalmente ni se ha dispuesto así en la tecnología para el análisis del contenido de las propias webs o del contenido de mensajes de las aplicaciones. Según el propietario del dispositivo se proporciona un reglamento estándar adaptado por el centro y aceptado posteriormente por las familias en el caso de menores.

El centro o los profesores que actúen como administradores, si están fuera del horario lectivo, pueden tomar acciones, pero no tendrán acceso a los dispositivos de los alumnos. A partir de la salida del colegio, velar por la seguridad del dispositivo, les corresponde a la familia.

19- Tenemos implantado Alexia en el centro, ¿existe la posibilidad de integrarse con IMTLazarus?

Efectivamente, tan solo es necesario que el colegio nos facilite lo que llamamos "datos de integración con Alexia" y a partir de ellos, se importan automáticamente los alumnos, los grupos de sección, los profesores y las familias, sincronizándose la información.

20- Nuestros profesores trabajan con Google Classroom, ¿es posible la integración con IMTLazarus?

Efectivamente, nos integramos con Google Classroom. IMTLazarus permite importar los grupos que necesita el profesor/a en cada momento, una vez finalizada la clase, puede mantenerlos en su Panel o eliminar el grupo.

21- Y si nuestra ERP es Educamos, ¿existe la posibilidad de integrarse con IMTLazarus?

Estamos en proceso de integración con Educamos.

22- Tengo mis claves de acceso a Google, ¿puedo acceder a IMTLazarus con mi cuenta de Google?

Si, siempre que sea la misma cuenta tanto en Google como en la plataforma IMTLazarus.

23- Tengo mis claves de acceso a Microsoft, ¿puedo acceder a IMTLazarus con mi cuenta de Microsoft?

Si, siempre que sea la misma cuenta de Azure. Es decir, solamente los del dominio podrían loguearse. No valdría usuario@outlook.com o @hotmail.com etc.

24- ¿Cómo se adquiere la solución y quien se encargaría de ponerlo en funcionamiento?

Se adquiere a través de un distribuidor certificado que le asesorará y se responsabilizará del proceso de implantación así como de la formación para su correcto uso y control.

25- He usado algunas apps de control parentales, ¿por qué es más interesante el uso de IMTLazarus?

IMTLazarus proporciona un entorno participativo con una seguridad variable en función de que el dispositivo esté dentro o fuera del colegio y quién tenga responsabilidad de actuar en él (personal del centro o familia), de forma que al gestionarse todo mediante una única aplicación se eliminan posibles conflictos por configuraciones llevadas a cabo entre los distintos supervisores, por ejemplo la restricción completa de cámara por parte de los padres desde casa, que imposibilite el llevar a cabo una actividad durante el horario escolar, etc.

26- ¿Puedo aplicar en remoto restricciones en el dispositivo de mi hijo?

Sí, IMTLazarus está diseñado específicamente para la gestión remota. Por lo que se podrá conectar a la aplicación desde cualquier dispositivo. Móvil, portátil, tablet,... siempre que disponga de conexión a Internet.

27- Como padre/madre de un menor, me preocupa el aspecto legal, ¿hasta qué punto se controla el dispositivo?

Las leyes garantizan la intimidad de los menores pero también obliga a los padres a velar por ellos. Hay que diferenciar entre el derecho de acceso y la información privada, los padres no podrán invadir la privacidad de sus hijos haciendo capturas de pantalla, viendo informes de navegación, a partir de los 15 años el sistema no debe estar dirigido a ver el contenido de lo que se está navegando, ni los mensajes que se están cruzando en las redes sociales, sino a controlar hábitos a la hora de acceder a determinadas webs. Como padres tendremos el derecho a decidir cuándo se puede o no conectar al dispositivo y que no pueda entrar a determinadas webs.

28- ¿Los padres/profesores pueden ver las navegaciones y las imágenes que se producen en el colegio/hogar?

El Administrador del centro educativo, encargado de IMTLazarus, está obligado a realizar una correcta configuración de los horarios y calendarios de entrada y salida del colegio. De modo que los profesores tendrán acceso a la navegación y las imágenes, exclusivamente en el horario lectivo, NUNCA fuera de ese horario. Por tanto será el profesor quien supervise los dispositivos durante ese tiempo, y cuando finalice, el profesor no podrá ver nada del alumno, será supervisado por su familia.

29- ¿Los profesores pueden enviar órdenes al dispositivo de mi hija fuera del horario escolar?

Los profesores han de ajustarse al calendario y horarios definidos por el centro, pero si un profesor envía órdenes al alumno fuera de ese horario, no se aplicarán hasta que no llegue la hora de entrada al colegio.

30- ¿Se aplica la seguridad en el dispositivo aunque los padres no entremos en la herramienta de forma regular?

Si, siempre que así lo hayan determinado el colegio y las familias estarán aplicadas las políticas de seguridad que tenga el centro las 24h.

31- ¿El servicio IMTLazarus sigue aplicándose en vacaciones?

Sí, el colegio renueva con IMTLazarus para el siguiente curso, no se parará el servicio durante las vacaciones, es decir, los alumnos mantendrán la protección, siempre que hayan contratado la licencia de 24h. Además, los padres pueden definir ciertas tareas que se ejecuten a una hora determinada, como por ejemplo desactivar automáticamente entre diario la navegación de internet a las 22:30, indicando que es momento de prepararse para descansar.

32- ¿Se guarda la información web en los servidores de IMTLazarus?, ¿cuánto tiempo?, ¿y las capturas de pantalla?

Sí, se guarda la información de navegación que se haya producido durante todo el curso escolar de todos los usuarios supervisados del colegio. En cuanto a las capturas de pantalla, se guardan los últimos 30 pantallazos. En cualquier caso, estas informaciones solamente pueden ser vistas por las familias, si se han obtenido fuera del horario escolar o por los educadores en caso de producirse en horario lectivo.

33- Distribuimos un software ERP, ¿lo podemos comunicar con IMTLazarus?, ¿cuáles son los pasos a seguir?

Deberá programar la comunicación con la API de IMTLazarus. Información disponible en la web oficial.

34- ¿Cómo puedo relacionar mi proyecto de software con IMTLazarus?

El servicio dispone de una API a través de la cual es posible sincronizar datos con aplicaciones de terceros como por ejemplo el ERP de una empresa o de un centro educativo.