Guía de uso básico de IMTLazarus

En este documento se expone el uso básico de IMTLazarus.
Dependiendo del perfil de supervisor se puede tener acceso a varias de las opciones que proporciona el sistema que se presenta a continuación. El número de acciones disponibles para cada supervisor dependerá de la administración del centro educativo.

Las funcionalidades son las siguientes:

- Acceso a la plataforma IMTLazarus
- Conexión y desconexión de Internet (individual y grupal)
- Filtrado personal
- Informes personalizados (individual y grupal)
- Control de cámara
- Información del dispositivo
- Cambio de contraseña

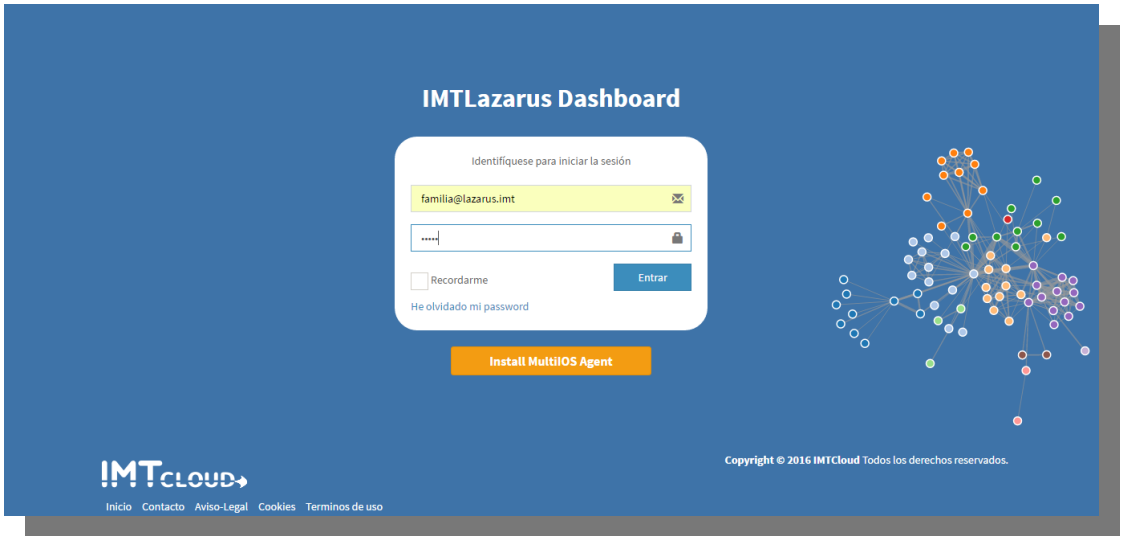
ACCIONES

1. **Validación**

   Cada supervisor contará con un USUARIO y una CONTRASEÑA para poder validarse en el sistema.

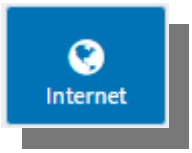
   La página web de gestión de dispositivos es la siguiente:

   http://[IDASIGNADO].imtlazarus.com/lazarus

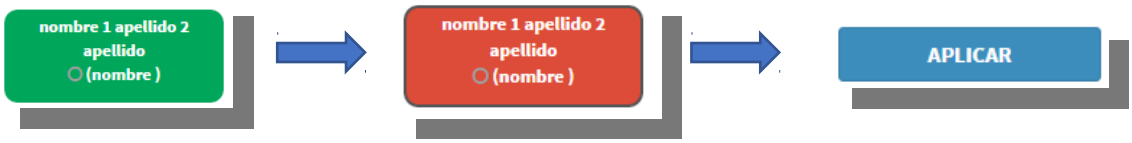


2. Conexión y desconexión de Internet

Los supervisores podrán limitar la conexión del dispositivo de manera indefinida y temporal.
Para ello solo tendrán que seguir este procedimiento.
Primero, deberán pulsar sobre el icono de “Internet” que aparece en la parte superior de la web.

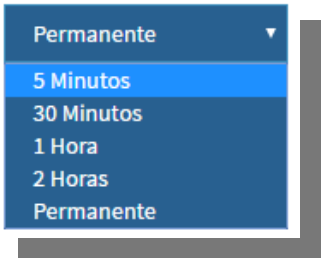


Por defecto los dispositivos tendrán habilitada la conexión a Internet, pero en un determinado momento el supervisor podrá limitar la misma. Para ello, solo tendrán que pulsar sobre el dispositivo hasta marcarlo en color rojo y darle a “aplicar”.
El estado en color verde representa el filtrado preestablecido por el colegio.

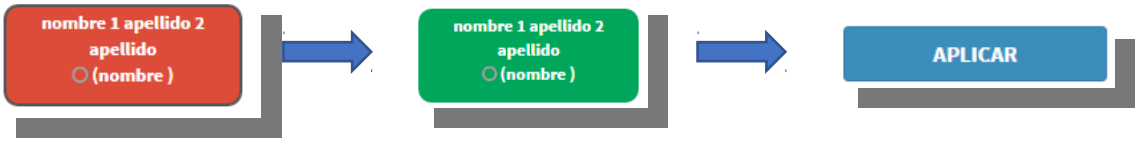


Una vez aplicada esta configuración, el dispositivo perderá la conexión a la red tanto para la navegación como para el uso de las aplicaciones instaladas en el mismo, si requieren de conexión.

Estas acciones pueden aplicarse de forma permanente (indefinida) o con una cuenta atrás, para esta segunda opción solo hay que elegir en el desplegable el tiempo de ejecución de la acción antes de pulsar “aplicar”.



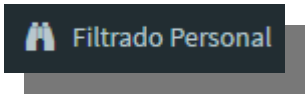
Para volver a tener conectividad en el dispositivo solo hay que revertir la acción anterior, (en lugar de poner el dispositivo en rojo ponerlo en verde), ya sea por un tiempo definido o de manera indefinida.



3. Filtrado personal

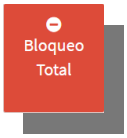
El filtrado personal permite elegir entre una serie de filtros preestablecidos para la aplicación en los dispositivos gestionados.

Para definir el filtrado personal que se le aplicará al dispositivo los supervisores tendrán que pulsar sobre la sección de filtrado personal en la parte izquierda de la web de gestión.



A continuación, podrán elegir el filtro de la navegación que más se ajuste a las necesidades de cada momento entre los disponibles en la plataforma.

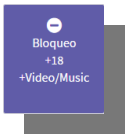
Los filtros son los siguientes:



Este filtrado bloquea completamente la navegación.

Este filtrado bloquea el contenido adulto (webs de sexo y de juego online), las redes sociales y las webs de visualización de audio y video.

Este filtrado bloquea el contenido adulto (webs de sexo y de juego online) y las redes sociales.



Este filtrado bloquea el contenido adulto (webs de sexo y de juego online) y las webs de visualización de audio y video.

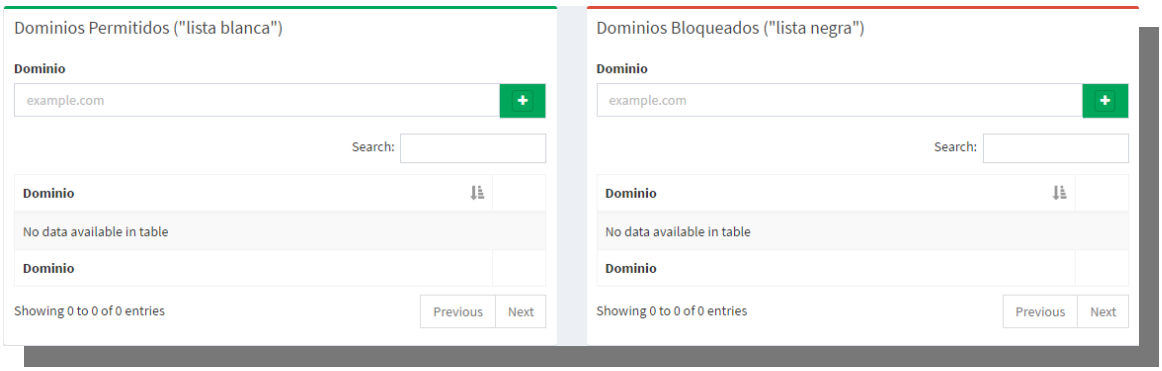
Este filtrado bloquea el contenido adulto (webs de sexo y de juego online).

Se seleccionará el filtrado a usar pulsando sobre el icono del mismo, en el momento que la configuración este guardada aparecerá un tic sobre el filtro en uso.

Además de los filtros preestablecidos, las familias que tengan varios hijos en colegios diferentes, podrán seleccionar un filtro de colegio que aplicará la misma configuración de filtrado en todos los dispositivos.

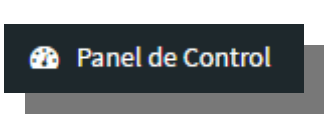
En esta misma sección se podrán establecer listas blancas y listas negras. Las webs introducidas en estas listas solo se aplicarán cuando este seleccionado el filtrado personal.

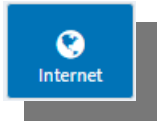
- **Lista blanca:** Las URLs introducidas en esta sección se saltarán cualquier filtrado de las listas seleccionadas.
- **Lista negra:** Las URLs introducidas en esta sección se bloquearán pese a que no pertenezca a ninguno de los filtros definidos.



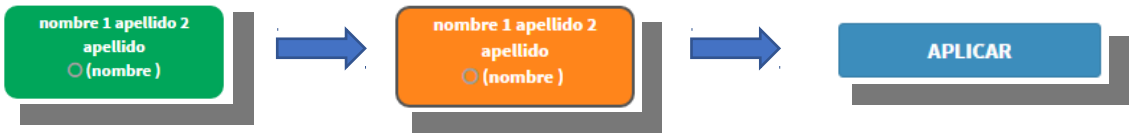
Para introducir URLs lo único que tendrán que hacer es escribir la dirección web a bloquear o permitir en el apartado elegido y pulsar sobre el icono +

Una vez seleccionado el filtro a aplicar e introducidas las URLs en la lista blanca y la lista negra, se podrán cargar sobre los dispositivos. Para ello primero deberán situarse en el apartado Internet de la misma manera que se ha hecho en la sección anterior "Conexión y desconexión de Internet" pulsando sobre la sección "Panel de Control" y a continuación sobre el icono "Internet".





Una vez en esta pantalla podrán pulsar sobre el dispositivo gestionado y dejarlo en el color naranja y a continuación pulsar "aplicar".



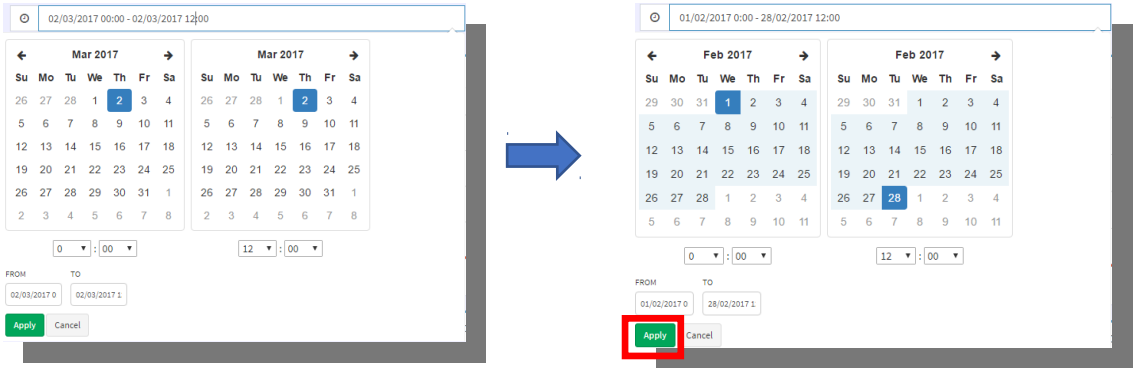
De la misma manera que en la sección anterior estas acciones podrán ser permanentes o temporales a la elección del supervisor.

Por último, para regresar a una configuración de libertad o de bloqueo se repetirán los pasos dejando el dispositivo en verde o en rojo.

4. Informes personalizados

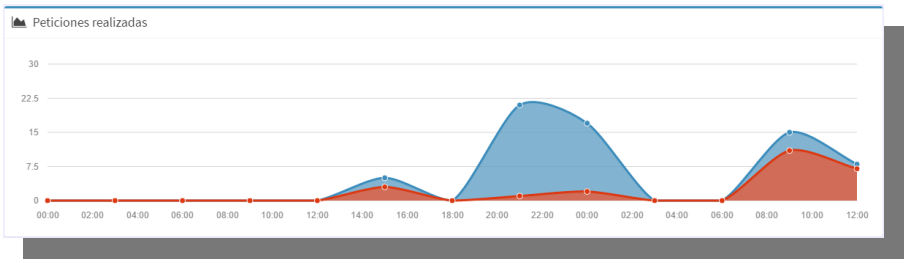
Los supervisores también podrán consultar la navegación realizada por los dispositivos desde el panel de IMTLazarus.
Para ello, deberán pulsar sobre el icono de “Informes” que aparece en la parte superior de la web.

Para la visualización de estas consultas pueden definirse periodos de tiempo como se muestra en la siguiente imagen, pulsando sobre la fecha en la parte superior izquierda.

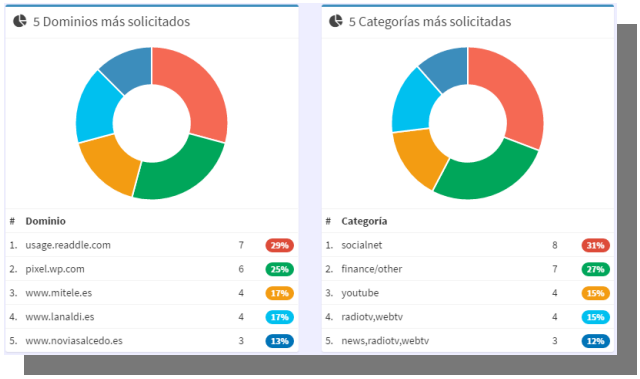


La pantalla de visualización de informes contiene varias secciones:

- La primera, como se muestra en la imagen, presenta una gráfica que indica la cantidad de peticiones (en AZUL las páginas a las que se ha intentado navegar, ya sea con el propio navegador o con alguna aplicación instalada en el dispositivo, y en ROJO las páginas bloqueadas por el sistema).

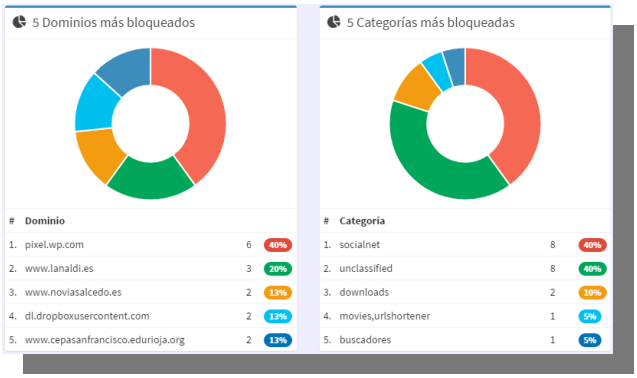


- A continuación, se ven dos gráficos que indican los dominios más visitados por el dispositivo y los grupos a los que pertenecen los mismos.



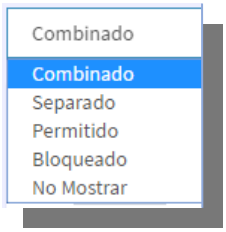
- En la misma línea, aparecen las palabras más usadas a la hora de navegar en el dispositivo.

- Los siguientes dos gráficos presentan las páginas más veces bloqueadas y los grupos a los que pertenecen las mismas.



Por último se pueden visualizar los dominios a los que ha navegado el dispositivo de manera desglosada por horarios.
Esta última representación puede ser mostrada de varias formas:

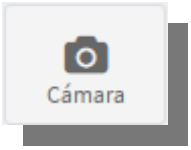
- Combinado > Muestra todos los dominios a los que ha accedido el dispositivo.
- Separado > Muestra los dominios por separado entre los permitidos y los bloqueados.
- Permitido > Solamente muestra los dominios a los que ha navegado el dispositivo y han sido permitidos por IMTLazarus.
- Bloqueado > Solamente muestra los dominios a los que ha navegado el dispositivo y han sido bloqueados por IMTLazarus.



5. Control de cámara

Los supervisores tendrán la opción de controlar el estado de la cámara de los dispositivos gestionados.

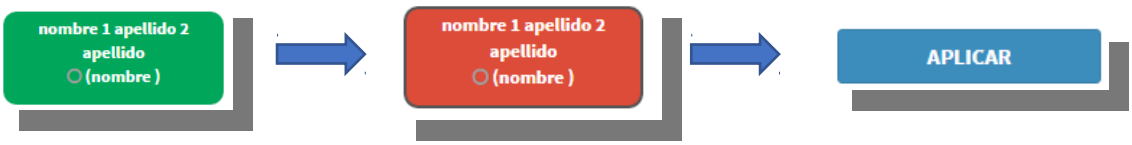
Para tomar medidas de supervisión sobre la cámara del dispositivo los supervisores tendrán que acceder a la sección “Cámara” situada en la parte superior.



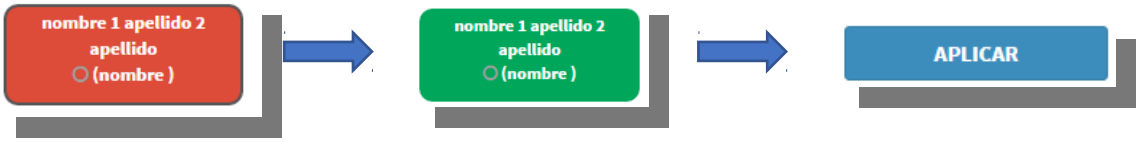
El control de cámara tiene dos estados ROJO (bloqueada) y VERDE (LIBRE).

Como en las secciones anteriores las acciones se podrán tomar de manera individualizada (pulsado sobre cualquier dispositivo) o de manera grupal (pulsando sobre los círculos de la parte superior).

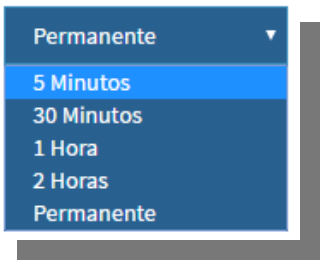
BLOQUEO



DESBLOQUEO



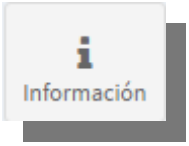
También se podrá definir un tiempo para la acción tomada utilizando el desplegable.



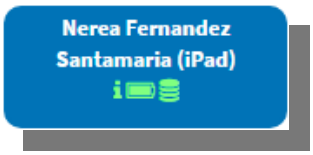
6. Información del dispositivo

Los supervisores tendrán la opción de visualizar información de sistema de los dispositivos asociados a la herramienta IMTLazarus.

Para acceder a esta sección tendrán que pinchar sobre el icono de "Información" situado en la parte superior de la plataforma de gestión.

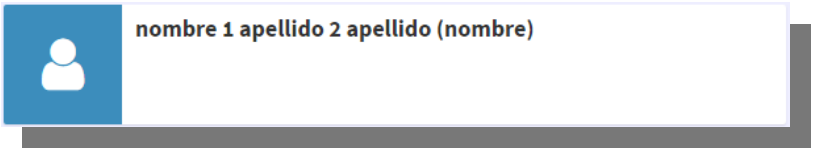


Para visualizar la información de sistema del dispositivo solo hay que pulsar el recuadro con el nombre del usuario que lo gestione.

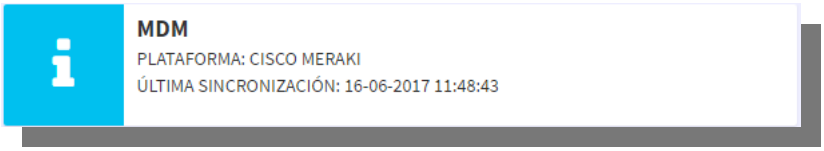


En la siguiente pantalla se podrá testear lo siguiente:

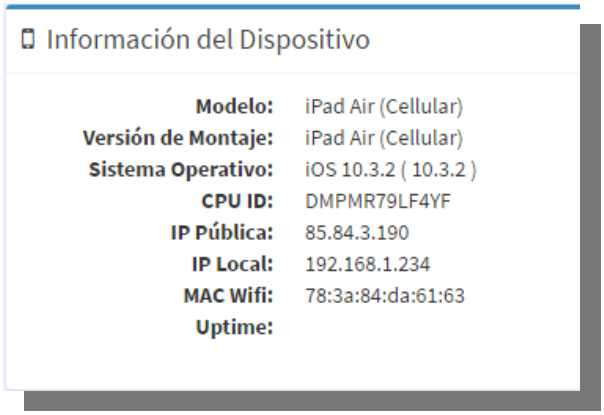
- Nombre y apellidos del usuario



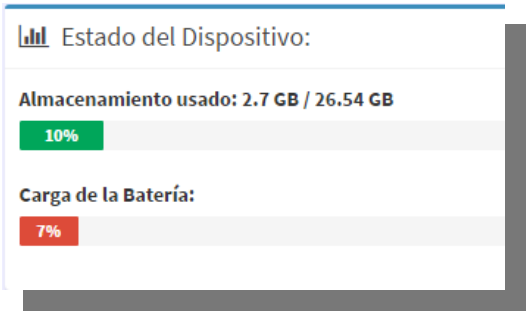
- Momento de la última sincronización con el MDM en caso de estar ligado a uno.



- Información detallada del sistema, Modelo del dispositivo, Versión del mismo, Sistema operativo instalado, CPU ID (número de serie), IP publica de la conexión, IP Local del dispositivo, MAC WIFI y Tiempo encendido.



- Estado de la memoria interna y la carga de la batería.

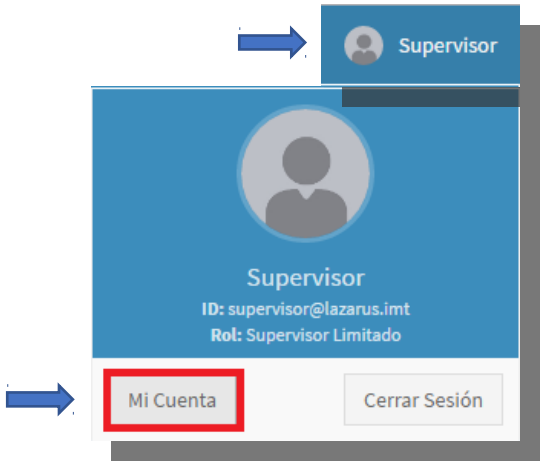


Dependiendo del sistema operativo la información obtenida por el sistema será una u otra.

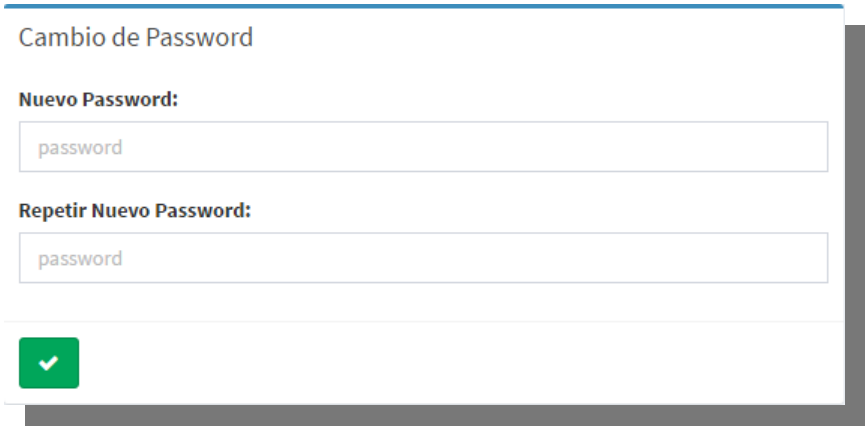
7. Cambio de contraseña

Es recomendable que todos los usuarios cambien su contraseña de acceso al panel de IMTLazarus al conectarse la primera vez. Para ello solo hay que seguir estos sencillos pasos.

- Se accede a la plataforma con el usuario y la contraseña proporcionados por el centro educativo.
- En la parte superior se pulsa sobre el nombre que identifica el usuario y en el desplegable sobre “Mi Cuenta”.



- En la pantalla que aparece al pulsar sobre el botón de “Mi Cuenta” podremos establecer una contraseña nueva además de cambiar ciertos datos como son el nombre y el apellido que aparecerán en la parte superior o el idioma en el que se cargara la página.



- Por ultimo recordar que para aplicar los cambios en la cuenta habrá que pulsar sobre el botón con el tic verde.