Carga de extensión IMTLazarus en Google Workspace y medidas de seguridad

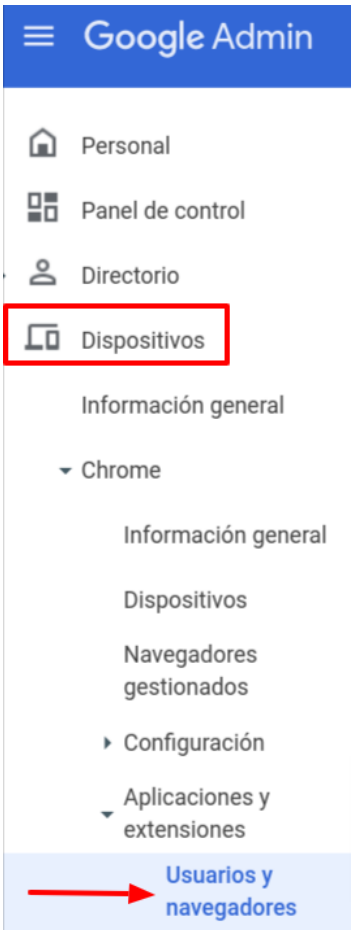
Índice

Introducción

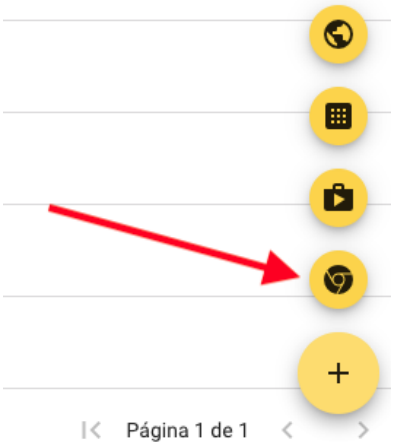
Para que IMTLazarus funcione correctamente en los dispositivos Chrome, IMTLazarus recomienda realizar las siguientes actuaciones dentro de la Consola de Administración de Google Workspace. El primer punto es obligatorio para que IMTLazarus funcione; los siguientes son recomendables para que los usuarios no puedan saltarse el filtrado:

1. Instalación de la extensión IMTLazarus:

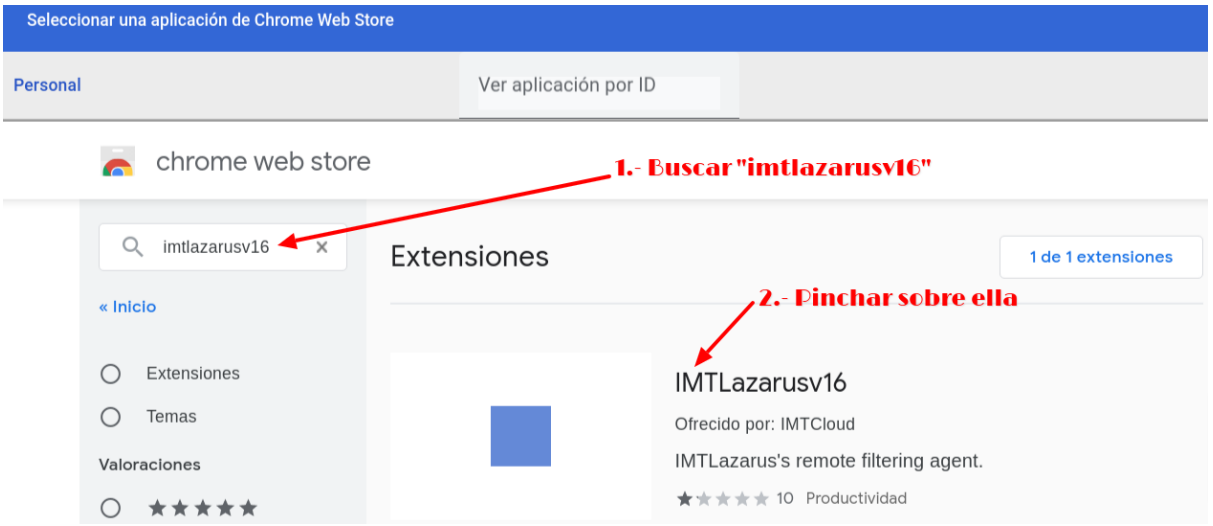
Desde la Consola de Administración de Google Workspace, en el menú de la izquierda, desplegamos el menú **Dispositivos > Chrome > Dispositivos Chrome Aplicaciones y extensiones y pinchamos en Usuarios y navegadores:**



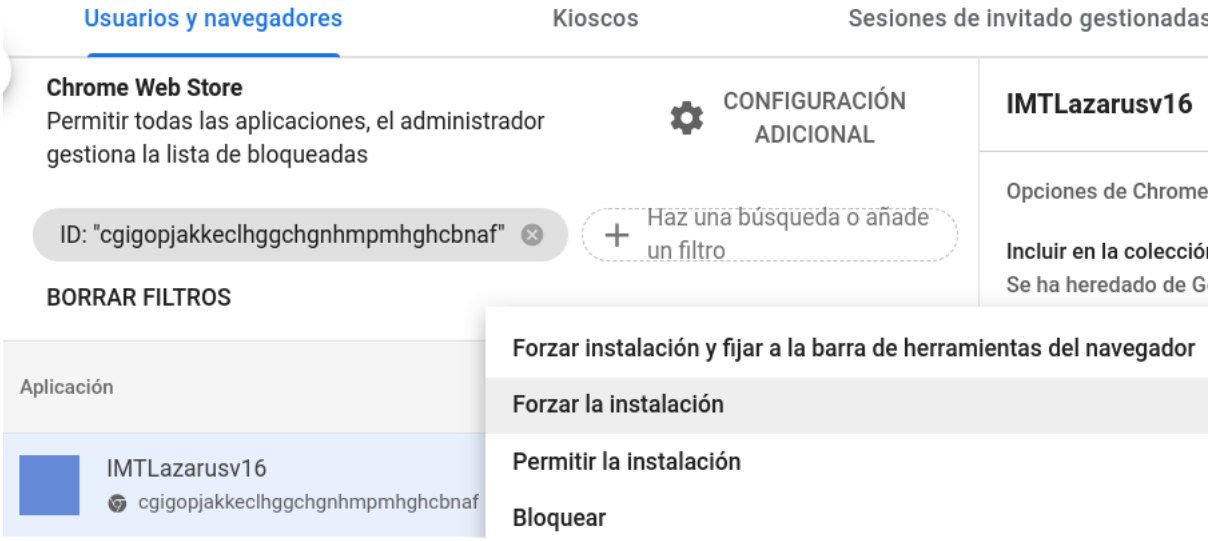
Una vez en esta pantalla, en la parte de la izquierda de la pantalla, seleccionaremos la Unidad Organizativa sobre la que queremos trabajar y, dentro de la pestaña de USUARIOS Y NAVEGADORES, le daremos al botón “+” amarillo que encontraremos abajo a la derecha y luego al icono de Chrome:



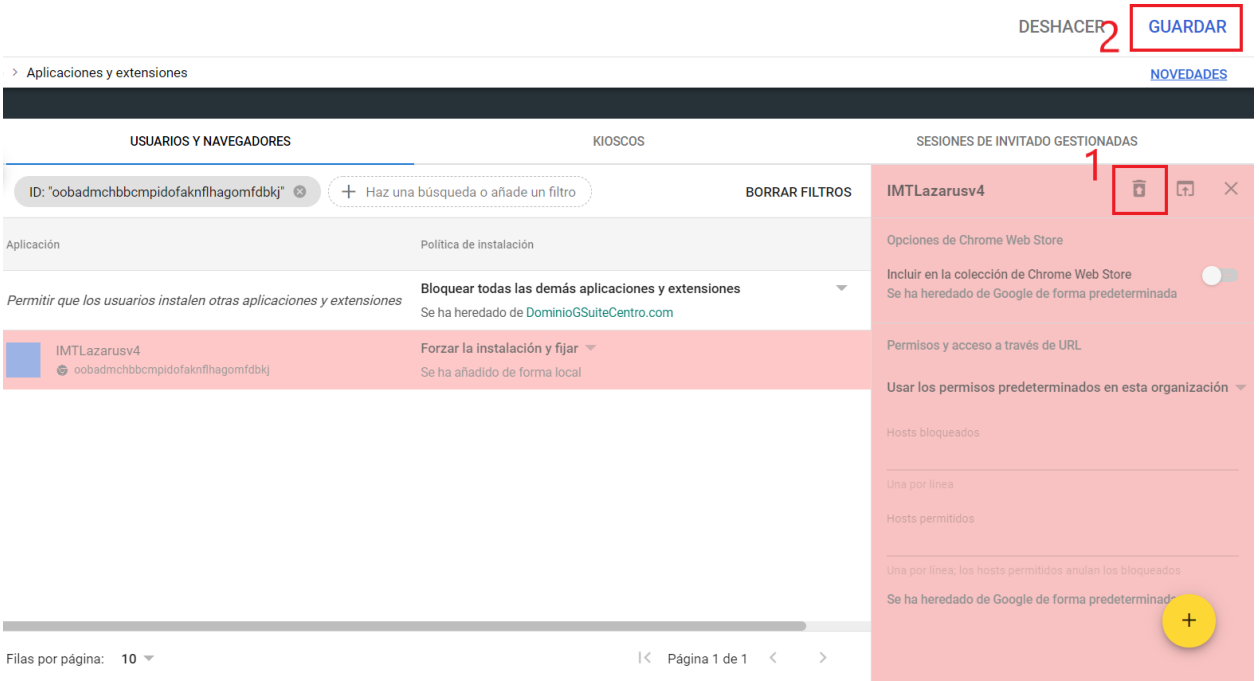
Esto hará que se nos abra una nueva ventana llamada “Seleccionar una aplicación de Chrome Web Store” desde la que tendremos que buscar la extensión **“IMTLazarusv16”**, pinchar sobre ella y después en **el botón azul de “Seleccionar”:**



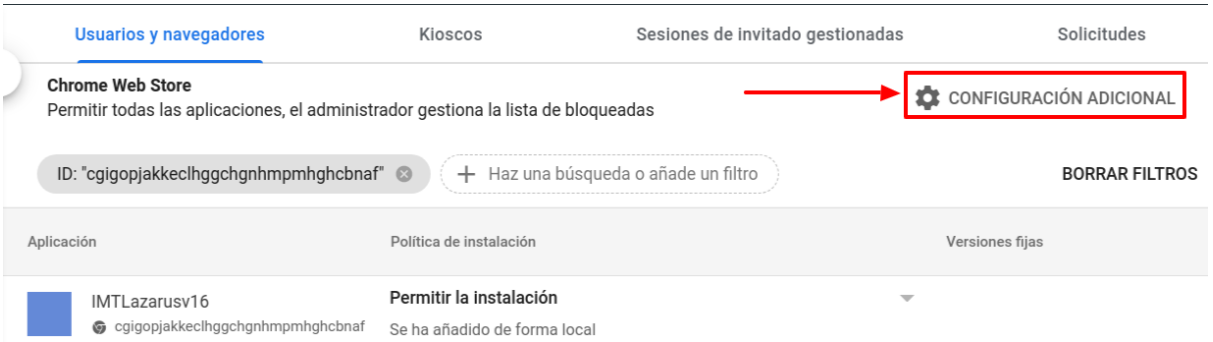
Una vez tengamos disponible la extensión, verificaremos que hemos seleccionado la Unidad Organizativa correcta y seleccionaremos como Política de instalación **"Forzar la instalación"** y le daremos al botón de **"GUARDAR"** que nos aparecerá arriba a la derecha de la pantalla.



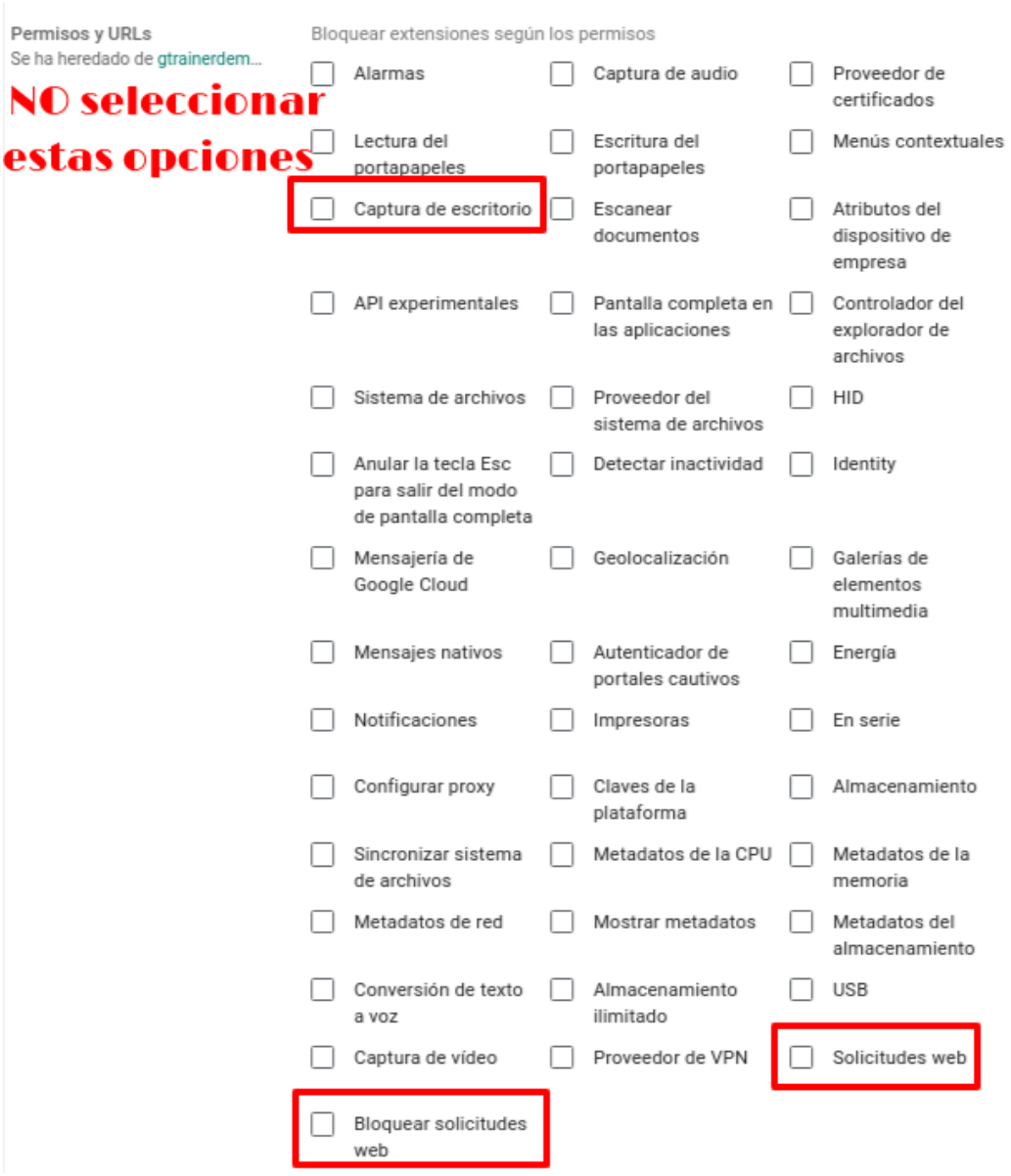
En el caso de tener instalada una versión anterior de la extensión de IMTLazarus, elimine dicha versión desde esta misma pantalla:



Sin salir de esa pantalla, pinchamos en la rueda dentada “Configuración Adicional”:



Dentro de la sección **“Configuración de aplicaciones adicional”**, dentro de “Permisos y URLs”, comprobamos que NO tenemos bloqueados los siguientes parámetros:

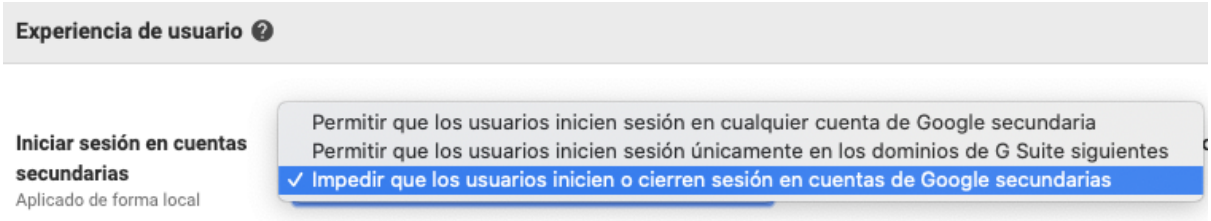


2. Impedir iniciar sesión con otras cuentas fuera del dominio y modo incógnito:

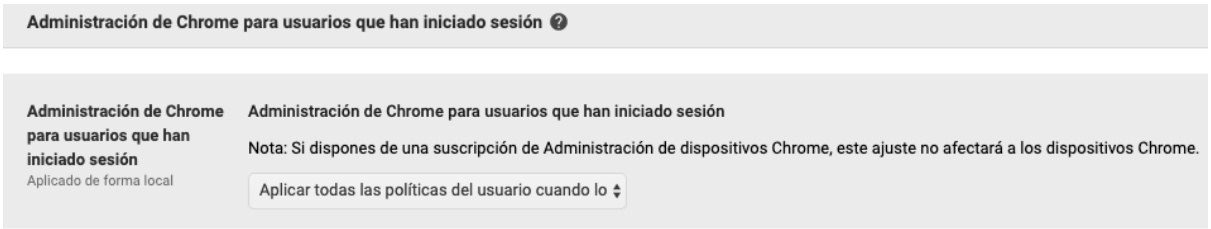
Desde la Consola de Administración de Google Workspace, en el menú de la izquierda, desplegamos el menú **Dispositivos > Chrome > Configuración y pinchamos en Usuarios y navegadores.**

Una vez en esta pantalla, en la parte de la izquierda de la pantalla, seleccionaremos la Unidad Organizativa sobre la que queremos trabajar.

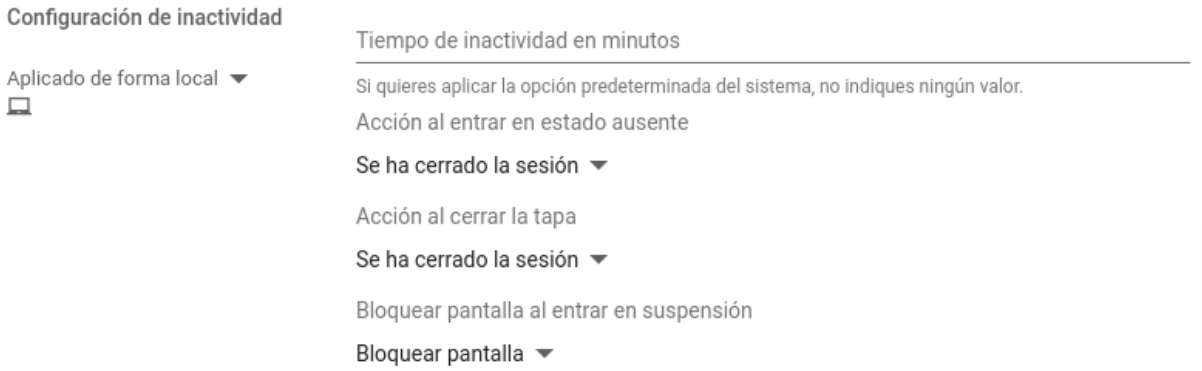
Dentro de esta pestaña de CONFIGURACIÓN DE USUARIO Y NAVEGADOR, iremos a la sección **Experiencia de usuario** y en **Iniciar sesión en cuentas secundarias** tendremos que pinchar y seleccionar la opción **"Impedir que los usuarios inicien o cierren sesión en cuentas de Google secundarias".** Para aplicar los cambios, le daremos al botón de **"GUARDAR"** que nos aparecerá arriba a la derecha de la pantalla.



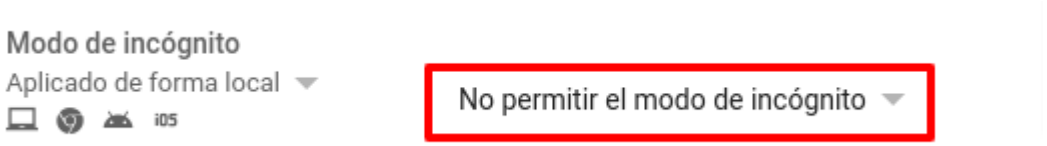
Sin salir de esa pantalla, en la sección **"Administración de Chrome para usuarios que han iniciado sesión"**, dentro de **Administración de Chrome para usuarios que han iniciado sesión** seleccionaremos la opción **"Aplicar todas las políticas del usuario cuando los usuarios inicien sesión en Chrome y proporcionar una experiencia gestionada de Chrome"**.



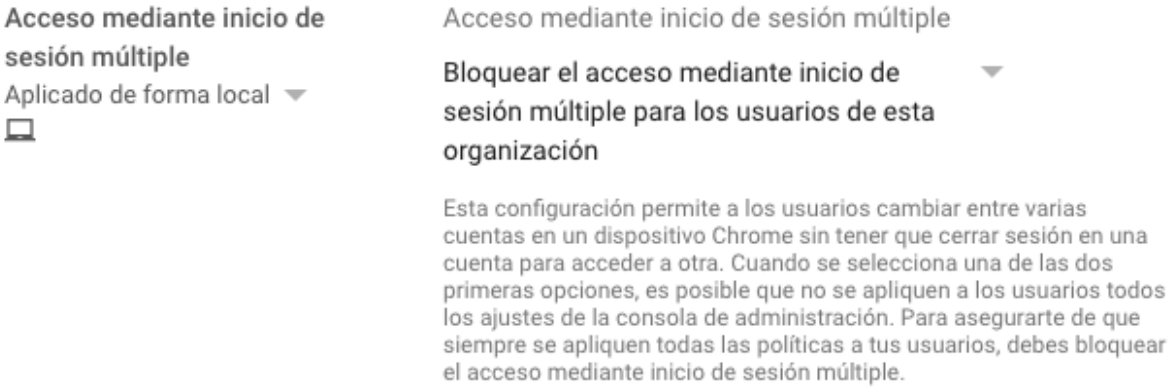
En la sección de **“Seguridad”** y en **Configuración de inactividad**, dentro de **“Bloquear pantalla cuando entre en suspensión”** seleccionaremos la opción de **“Bloquear pantalla”:**



Justo debajo de ese parámetro y dentro de esa misma sección de Seguridad, en **Modo de incógnito** seleccionaremos la opción **“No permitir el modo de incógnito”** y le daremos al botón de **“GUARDAR”** que nos aparecerá arriba a la derecha de la pantalla.

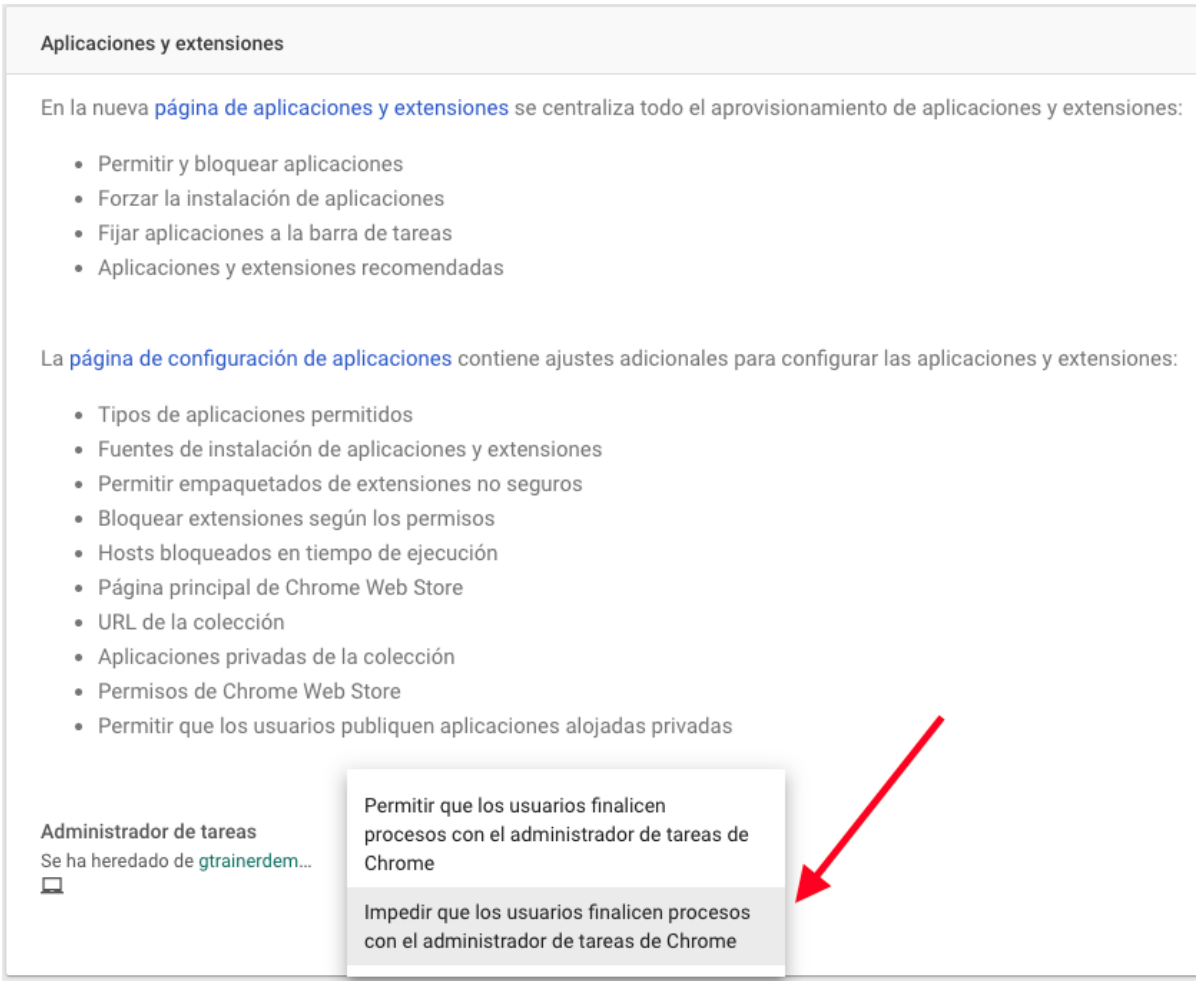


Sin salir de donde estamos en la pestaña de CONFIGURACIÓN DE USUARIO Y NAVEGADOR, iremos a la sección **Experiencia de usuario** y en **Acceso mediante inicio de sesión múltiple** seleccionaremos la opción **“Bloquear el acceso mediante inicio de sesión múltiple para usuario de esta organización”** y le daremos al botón de **“GUARDAR”** que nos aparecerá arriba a la derecha de la pantalla.



3. Impedir que los usuarios finalicen procesos con el administrador de tareas de Chrome:

Sin salir de la pestaña de CONFIGURACIÓN DE USUARIO Y NAVEGADOR, iremos a la sección **Aplicaciones y extensiones** y en **Administrador de tareas** seleccionaremos la opción **"Impedir que los usuarios finalicen procesos con el administrador de tareas de Chrome"** y le daremos al botón de **"GUARDAR"** que nos aparecerá arriba a la derecha de la pantalla.



4. Permisos de registro de los equipos:

Para evitar que los usuarios reestablezcan los dispositivos a el estado de fábrica y, por tanto, desinstalen IMTLazarus y cualquier otra aplicación, es necesario que activemos el registro obligatorio del equipo, para que así, si esto ocurriese (el reseteo o “powerwash” del dispositivo Chrome), obligue a enrolarlo en la Consola de Administración para poder utilizarlo.
Para ello, en la Consola de Administración de Google Workspace, en el menú de la izquierda, desplegamos el menú **Dispositivos > Chrome > Configuración y pinchamos en Usuarios y navegadores.**

Una vez en esta pantalla, en la parte de la izquierda de la pantalla, seleccionaremos la Unidad Organizativa sobre la que queremos trabajar.

Dentro de esta pestaña de CONFIGURACIÓN DE USUARIO Y NAVEGADOR, iremos a la sección **Controles de registro**, configura el ajuste **Permisos de registro** como: **No permitir que los usuarios de esta organización registren dispositivos nuevos o que ya hayan estado registrados anteriormente.**
Le daremos al botón de “Guardar” que aparecerá en la parte superior derecha de la pantalla.

Sin salir de donde estamos, en la pestaña de CONFIGURACIÓN DEL DISPOSITIVO, iremos a la sección **Registro y acceso** y marcaremos lo siguiente:

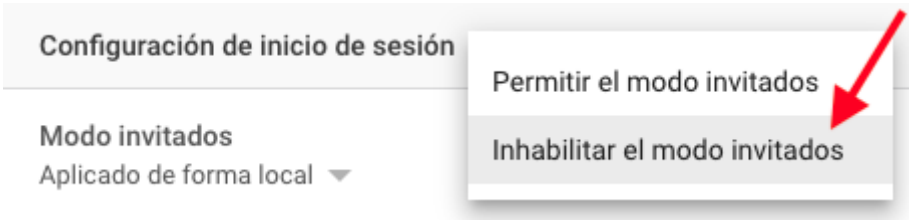
- **Obligación de volver a realizar el registro:** Forzar la repetición del registro del dispositivo con las credenciales del usuario cuando se borren sus datos
- **Powerwash:** No permitir que se active la función Powerwash

Le daremos al botón de “Guardar” que aparecerá en la parte superior derecha de la pantalla.

De esta forma, si un usuario restablece los valores de fábrica, tendrá que devolvernos el dispositivo para que lo volvamos a enrolar manualmente con una cuenta de Administrador.

5. Impedir iniciar sesión como invitado:

Desde la misma ventana, pincharemos en la pestaña de CONFIGURACIÓN DEL DISPOSITIVO, iremos a la sección **Configuración de inicio de sesión** y en **Modo invitados** seleccionaremos la opción **"Inhabilitar el modo invitados"** y le daremos al botón de **"GUARDAR"** que nos aparecerá arriba a la derecha de la pantalla.



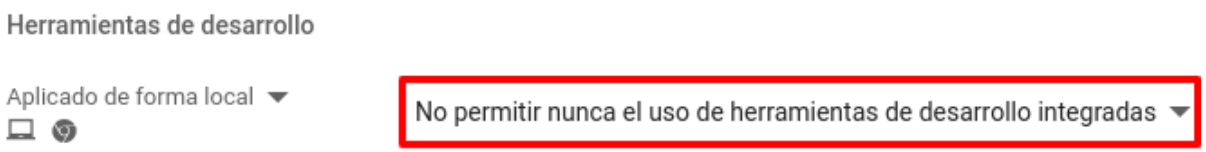
Si nos hemos salido de la pantalla, podremos volver a la pantalla principal de la Consola de Administración y, en el menú de la izquierda, desplegamos el menú **Dispositivos > Chrome > Configuración y pinchamos en Dispositivo.**
Seleccionaremos la Unidad Organizativa donde queremos aplicar los cambios. Buscamos la sección llamada **Configuración de inicio de sesión** y en el parámetro **"Modo invitados"** marcamos **"Inhabilitar el modo invitados"**. Para guardar los cambios, le daremos al botón de Guardar que nos aparecerá arriba a la derecha de la pantalla.

6. Impedir modo desarrollador:

Desde la Consola de Administración de Google Workspace, en el menú de la izquierda, desplegamos el menú **Dispositivos > Chrome > Configuración y pinchamos en Usuarios y navegadores.**

Una vez en esta pantalla, en la parte de la izquierda de la pantalla, seleccionaremos la Unidad Organizativa sobre la que queremos trabajar.

Buscamos la sección llamada **Experiencia de usuario** y en el parámetro **"Herramientas de desarrollo"** seleccionamos **"No permitir nunca el uso de herramientas de desarrollo integradas"**. Para guardar los cambios, le daremos al botón de Guardar que nos aparecerá arriba a la derecha de la pantalla:



7. Desactivar la app cámara para controlar el uso de cámara en sesiones de Google Meet:

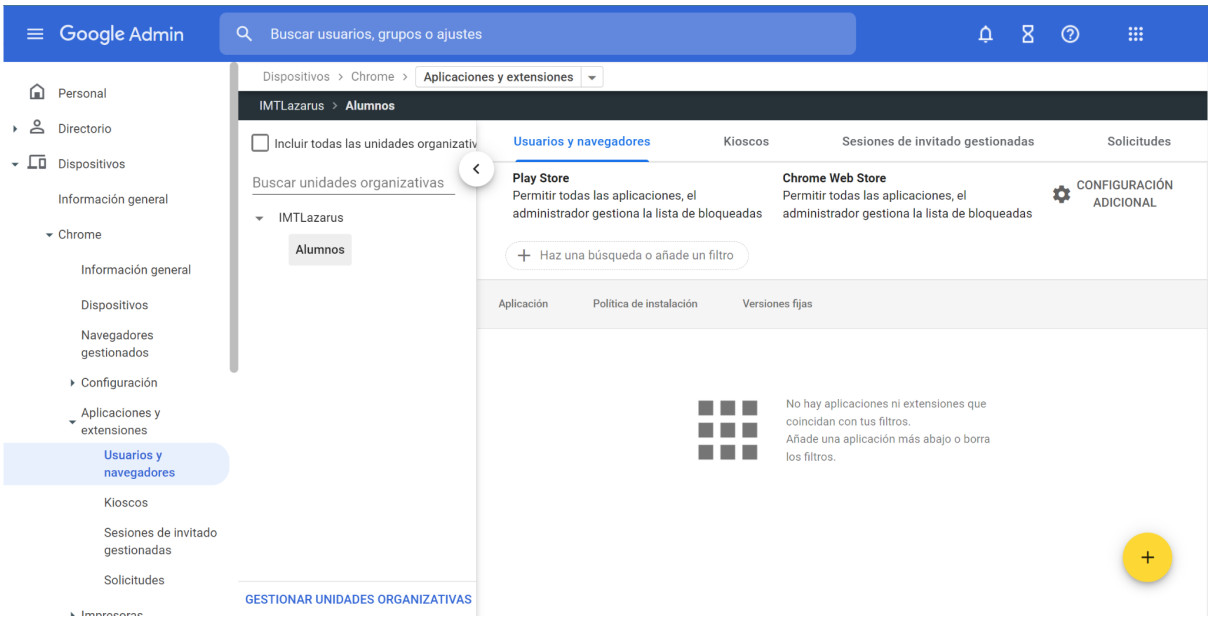
Desde la Consola de Administración de Google Workspace, podemos deshabilitar tanto el recurso de la cámara a nivel de Hardware (se desactiva por completo) ó restringir la aplicación nativa de la cámara, pero a su vez permitir su uso en sesiones de Google Meet y permitir a los supervisores controlarla desde IMTLazarus con la funcionalidad “Google Meet - Inside!”.

Para restringir la cámara desde la Consola, necesitaremos conocer el ID de la aplicación de la cámara. Desde Chrome Web Store la localizamos en la siguiente URL:

https://chrome.google.com/webstore/detail/camera/**hfhhnacclhffhdffklopdkcgdhifgngh**

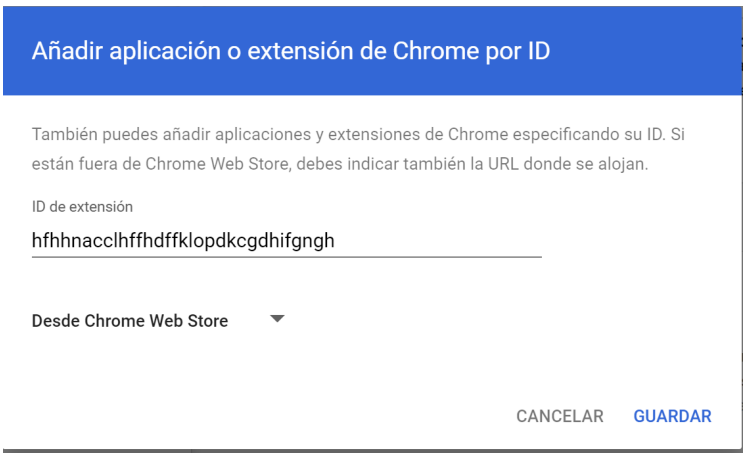
Nos quedamos con la parte final del ID: **hfhhnacclhffhdffklopdkcgdhifgngh**

Desde la Consola de Administración de Google Workspace, en el menú de la izquierda, desplegamos el menú **Dispositivos > Chrome > Aplicaciones y extensiones > Usuarios y navegadores.** Seleccionamos la **Unidad Organizativa** donde queramos aplicar la restricción.

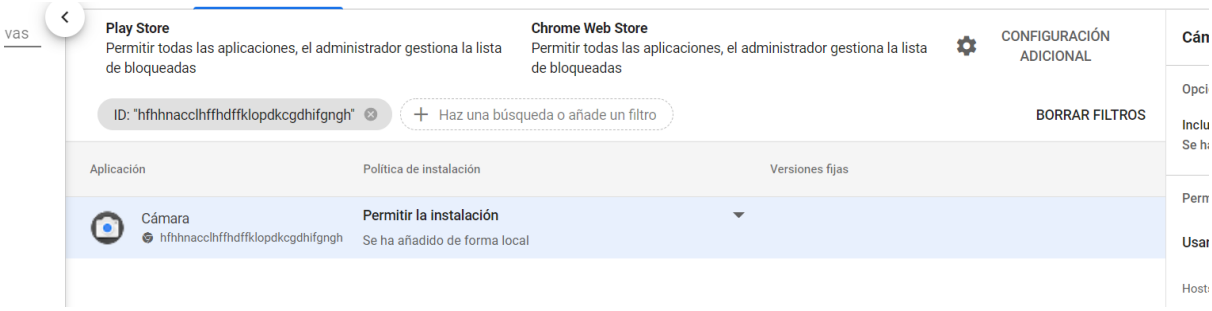


Pulsamos en el **Botón + amarillo > Añadir aplicación o extensión de Chrome por ID**

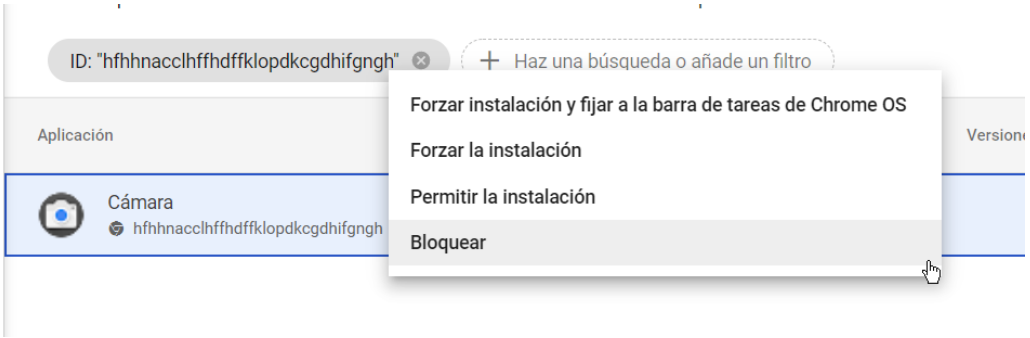
En la ventana que se abre, introducimos el ID de la aplicación de la cámara que hemos obtenido anteriormente: **hfhhnacclhffhdffklopdkcgdhifgngh** y pulsamos **GUARDAR**



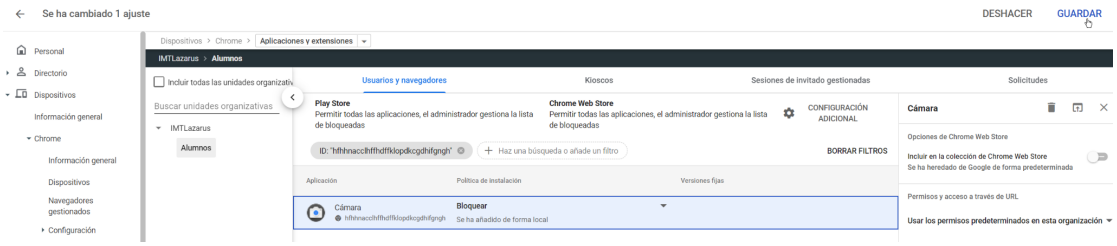
Una vez añadida:



Pulsamos en el desplegable y seleccionamos **“Bloquear”**



Y por último pulsamos **GUARDAR** en la parte superior derecha de la pantalla.

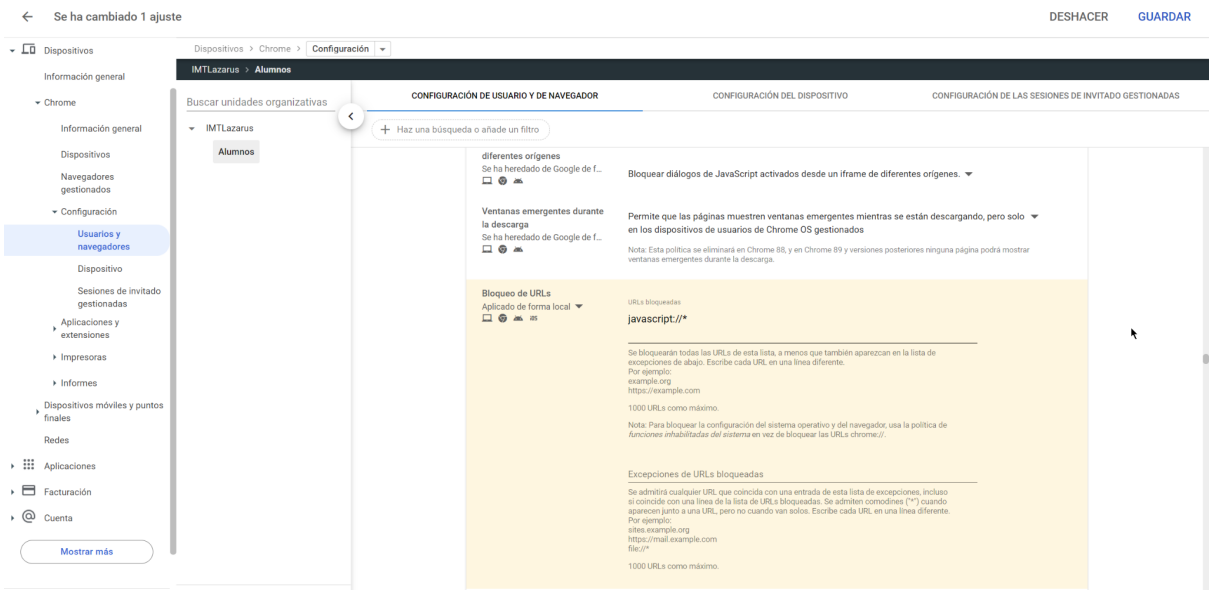


8. Desactivar la ejecución de javascript en la barra del navegador:

Para prevenir que los alumnos puedan hacer uso de expresiones javascript para intentar saltarse el bloqueo, debemos añadir una configuración adicional.

Desde la Consola de Administración de Google Workspace, en el menú de la izquierda, desplegamos el menú **Dispositivos > Chrome > Configuración y pinchamos en Usuarios y navegadores.** Seleccionamos la **Unidad Organizativa** donde queramos aplicar la restricción.

En **Bloqueo de URLs** añadimos **javascript://*** y pulsamos **GUARDAR** en la parte superior.

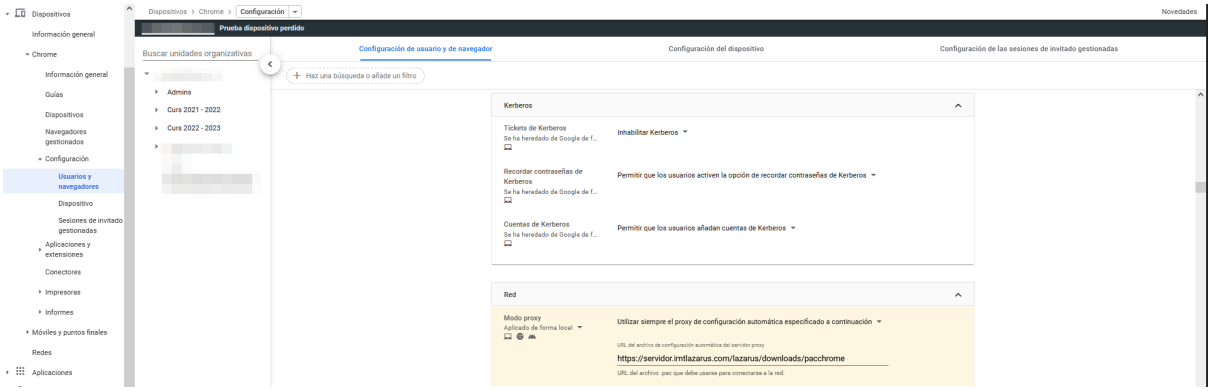


9. PAC para seguridad en el acceso a Play Store:

Para garantizar la seguridad de los dispositivos al acceder a la Play Store, debemos configurar el siguiente parámetro desde la Consola:

Desde la Consola de Administración de Google Workspace, en el menú de la izquierda, desplegamos el menú **Dispositivos > Chrome > Configuración y pinchamos en Usuarios y navegadores.** Seleccionamos la **Unidad Organizativa** donde queramos aplicar la restricción.

En la sección de **Red**, dentro del parámetro **“Modo proxy”** seleccionamos la opción **“Utilizar siempre el proxy de configuración automática especificado a continuación”:** y añadimos la siguiente URL: https://server.imtlazarus.com/lazarus/downloads/pacchrome



Y por último pulsamos **GUARDAR** en la parte superior derecha de la pantalla.