Index

# Introduction

So that IMTLazarus works correctly on Chrome devices, IMTLazarus recommends performing the following actions within the Google Workspace Admin Console. The first point is mandatory so that IMTLazarus work; The following are recommended so that users cannot bypass filtering:
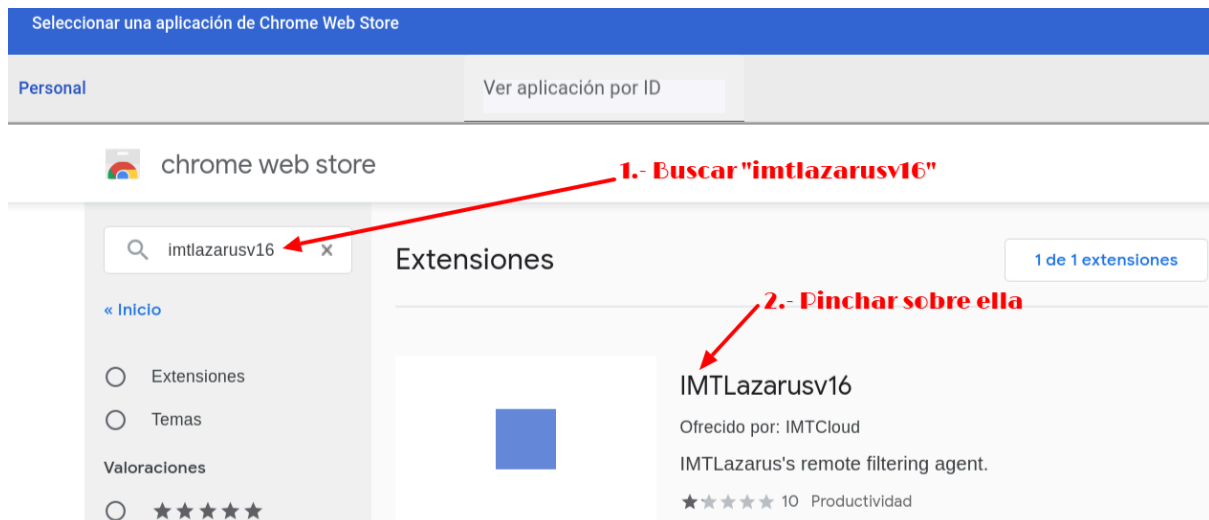
1. Installation of the extension IMTLazarus:

From the Google Workspace Administration Console, in the menu on the left, we display the menu **Devices > Chrome > Chrome Devices Applications and extensions and click on Users and browsers:**
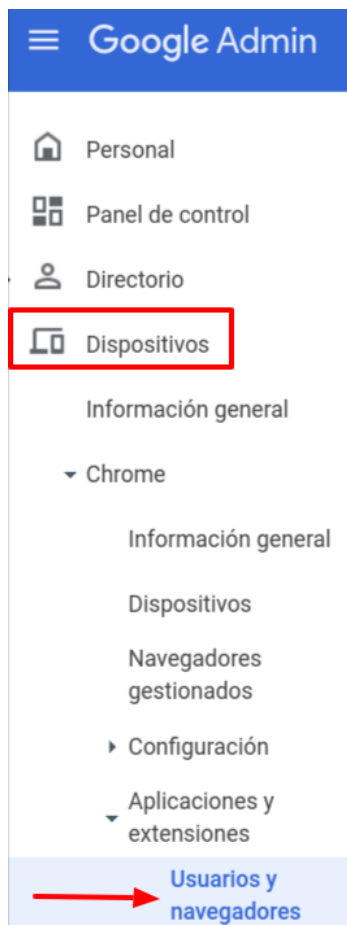
Once on this screen, on the left side of the screen, <u>We will select the Organizational Unit on which we want to work</u> and, within the USERS AND BROWSERS tab, we will click on the yellow "+" button that we will find at the bottom right and then on the Chrome icon:
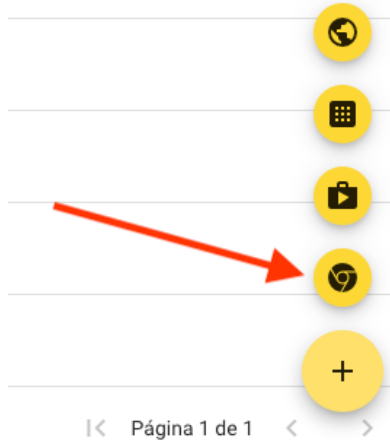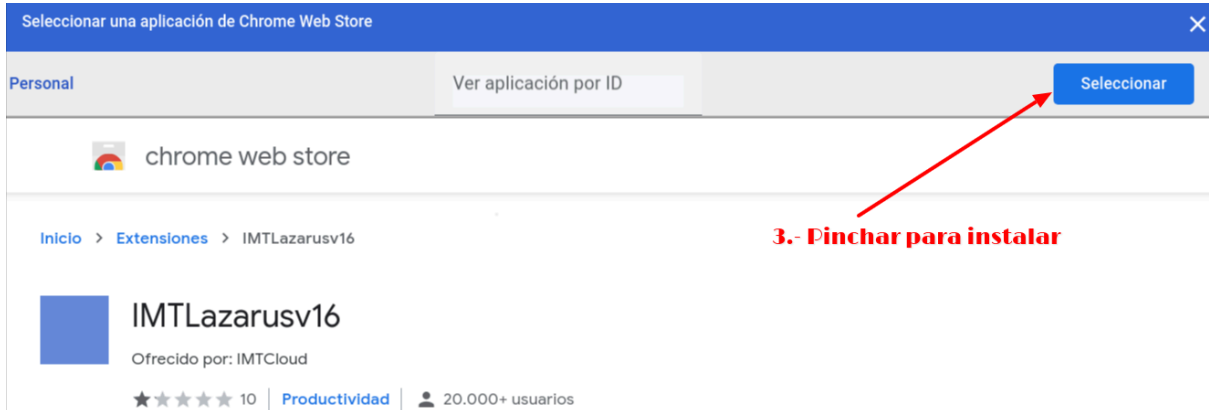

This will open a new window called "Select an application from the Chrome Web Store" from which we will have to search for the extension **"IMTLazarusv16"**, click on it and then on **the blue "Select" button:**
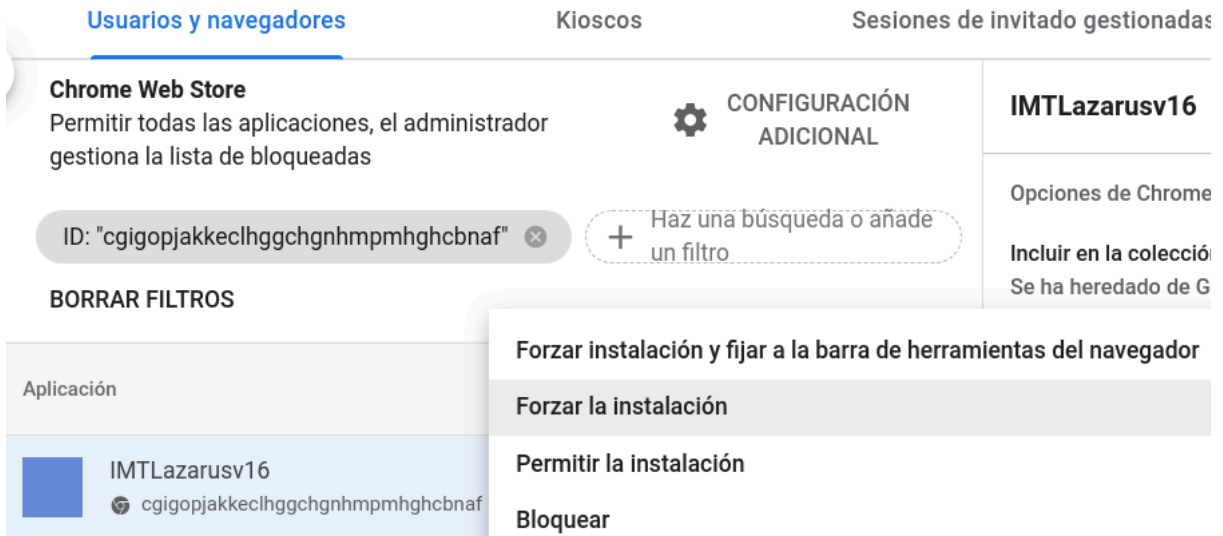
3.- Pinchar para instalar

Once we have the extension available, we will verify that we have selected the correct Organizational Unit and we will select the Installation Policy **"Force installation"** and we will hit the button **"KEEP"** that will appear at the top right of the screen.

If you have a previous version of the IMTLazarus extension installed, delete said version from this same screen:

Without leaving that screen, click on the "Additional Configuration" gear:
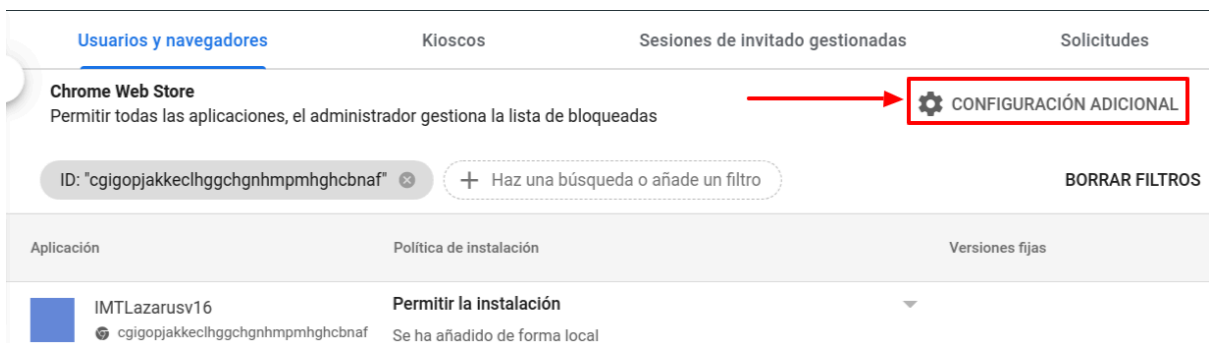
Inside the section **"Additional application settings"**, within "Permissions and URLs", we check that we DO NOT have the following parameters blocked:

Permisos y URLs
Se ha heredado de gtrainerdem...

NO seleccionar estas opciones

Bloquear extensiones según los permisos

|		
☐ Alarmas	☐ Captura de audio	☐ Proveedor de certificados
☐ Lectura del portapapeles	☐ Escritura del portapapeles	☐ Menús contextuales
☐ Captura de escritorio	☐ Escanear documentos	☐ Atributos del dispositivo de empresa
☐ API experimentales	☐ Pantalla completa en las aplicaciones	☐ Controlador del explorador de archivos
☐ Sistema de archivos	☐ Proveedor del sistema de archivos	☐ HID
☐ Anular la tecla Esc para salir del modo de pantalla completa	☐ Detectar inactividad	☐ Identity
☐ Mensajería de Google Cloud	☐ Geolocalización	☐ Galerías de elementos multimedia
☐ Mensajes nativos	☐ Autenticador de portales cautivos	☐ Energía
☐ Notificaciones	☐ Impresoras	☐ En serie
☐ Configurar proxy	☐ Claves de la plataforma	☐ Almacenamiento
☐ Sincronizar sistema de archivos	☐ Metadatos de la CPU	☐ Metadatos de la memoria
☐ Metadatos de red	☐ Mostrar metadatos	☐ Metadatos del almacenamiento
☐ Conversión de texto a voz	☐ Almacenamiento ilimitado	☐ USB
☐ Captura de vídeo	☐ Proveedor de VPN	☐ Solicitudes web
☐ Bloquear solicitudes web		

# 2. Prevent logging in with other accounts outside the domain and incognito mode:

From the Google Workspace Administration Console, in the menu on the left, we display the menu **Devices > Chrome > Settings and click on Users and browsers.**

Once on this screen, on the left side of the screen, <u>We will select the Organizational Unit on which we want to work</u>.

Within this USER AND BROWSER SETTINGS tab, we will go to the section **User experience** and in **Sign in to secondary accounts** we will have to click and select the option **"Prevent users from signing in or out of secondary Google accounts."** To apply the changes, we will click on the button **"KEEP"** that will appear at the top right of the screen.
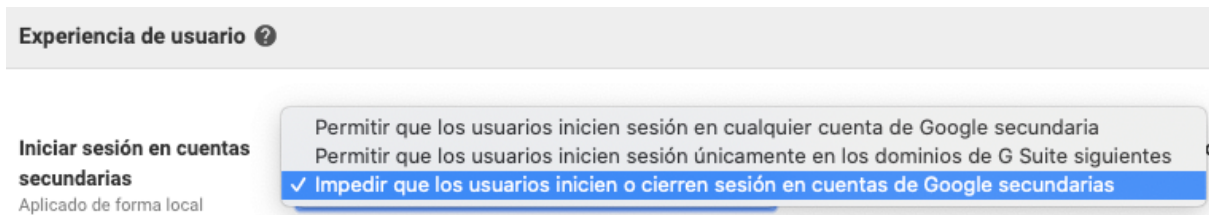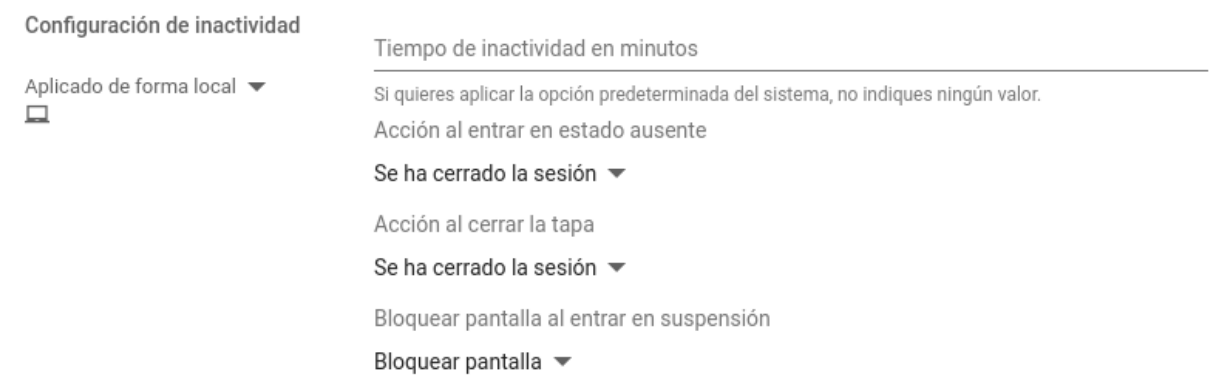

Without leaving that screen, in the section **"Chrome administration for users who are logged in"**, within **Chrome administration for users who are logged in** we will select the option **"Enforce all user policies when users sign in to Chrome and provide a managed Chrome experience"**.
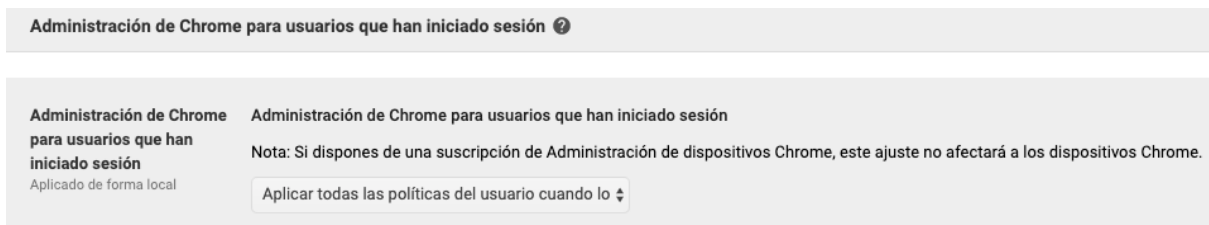
In the section of **"Security"** and in **Idle Settings**, within **"Lock screen when it goes to sleep"** We will select the option **"Lock screen"**:

Configuración de inactividad

Aplicado de forma local ▼

Tiempo de inactividad en minutos

Si quieres aplicar la opción predeterminada del sistema, no indiques ningún valor.

Acción al entrar en estado ausente
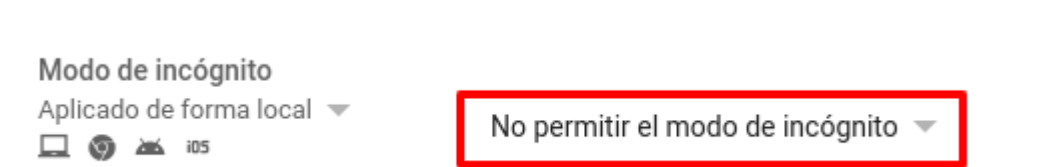
Se ha cerrado la sesión ▼

Acción al cerrar la tapa

Se ha cerrado la sesión ▼

Bloquear pantalla al entrar en suspensión

Bloquear pantalla ▼

Just below that parameter and within that same Security section, in **incognito mode** we will select the option **"Do not allow incognito mode"** and we will hit the button **"KEEP"** that will appear at the top right of the screen.
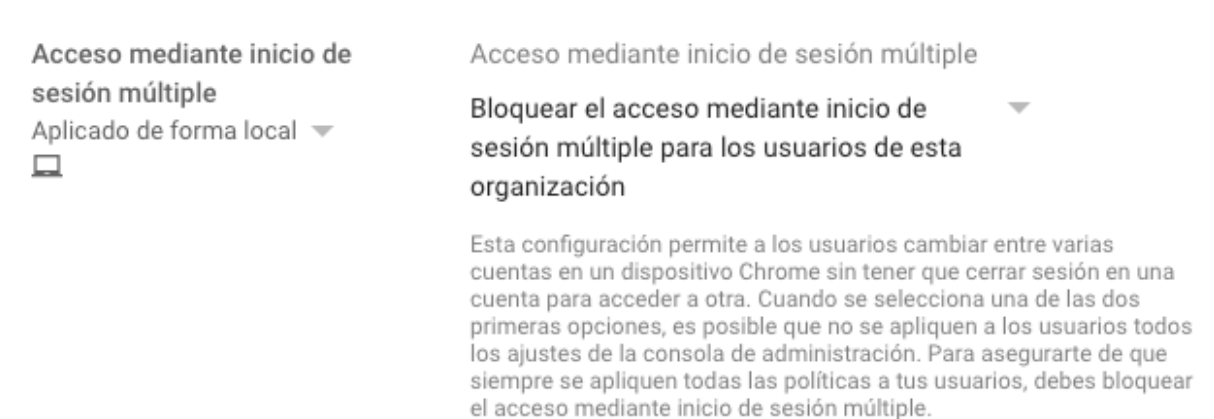
Modo de incógnito

Aplicado de forma local ▼

No permitir el modo de incógnito ▼

Without leaving where we are in the USER AND BROWSER SETTINGS tab, we will go to the section **User experience** and in **Multiple login access** we will select the option **"Block multiple sign-in access for a user in this organization"** and we will hit the button **"KEEP"** that will appear at the top right of the screen.

Acceso mediante inicio de sesión múltiple

Aplicado de forma local ▼

Acceso mediante inicio de sesión múltiple

Bloquear el acceso mediante inicio de sesión múltiple para los usuarios de esta organización ▼

Esta configuración permite a los usuarios cambiar entre varias cuentas en un dispositivo Chrome sin tener que cerrar sesión en una cuenta para acceder a otra. Cuando se selecciona una de las dos primeras opciones, es posible que no se apliquen a los usuarios todos los ajustes de la consola de administración. Para asegurarte de que siempre se apliquen todas las políticas a tus usuarios, debes bloquear el acceso mediante inicio de sesión múltiple.

3. Prevent users from ending processes with Chrome task manager:

Without leaving the USER AND BROWSER SETTINGS tab, we will go to the section **Apps and extensions** and in **Task Manager** we will select the option **"Prevent users from ending processes with the Chrome task manager"** and we will hit the button **"KEEP"** that will appear at the top right of the screen.

4. Equipment registration permissions:

To prevent users from resetting the devices to the factory state and, therefore, uninstalling IMTLazarus and any other application, it is necessary that we activate the mandatory registration of the device, so that if this occurs (the reset or "powerwash" of the Chrome device), force you to enroll it in the Administration Console in order to use it.
To do this, in the Google Workspace Administration Console, in the menu on the left, we display the menu **Devices > Chrome > Settings and click on Users and browsers.**

Once on this screen, on the left side of the screen, We will select the Organizational Unit on which we want to work.

Within this USER AND BROWSER SETTINGS tab, we will go to the section **Registration controls**, configure the setting **Registration permissions** as: **Do not allow users in this organization to register new or previously registered devices.**
We will click on the "Save" button that will appear in the upper right part of the screen.

Without leaving where we are, in the DEVICE SETTINGS tab, we will go to the section **Registration and access** and we will mark the following:

- **Obligation to re-register:** Force device re-registration with user credentials when user data is wiped
- **Powerwash:** Do not allow the Powerwash function to activate

We will click on the "Save" button that will appear in the upper right part of the screen.

This way, if a user performs a factory reset, they will need to return the device to us for manual re-enrollment with an Administrator account.

5. Prevent logging in as a guest:

From the same window, we will click on the DEVICE SETTINGS tab, we will go to the section **Login settings** and in **Guest mode** we will select the option **"Disable guest mode"** and we will hit the button **"KEEP"** that will appear at the top right of the screen.
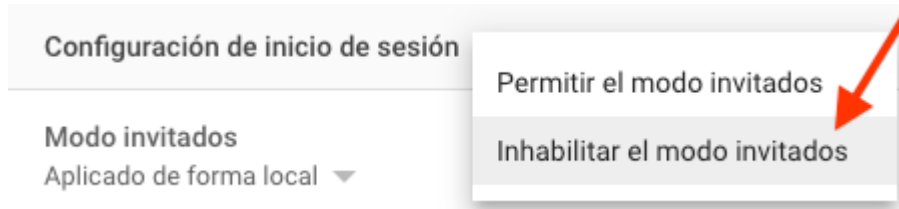
If we have left the screen, we can return to the main screen of the Administration Console and, in the menu on the left, we display the menu **Devices > Chrome > Settings and click on Device.**

We will select the Organizational Unit where we want to apply the changes. We look for the section called **Login settings** and in the parameter **"Guest mode"** we mark **"Disable guest mode"**. To save the changes, we will click on the Save button that will appear at the top right of the screen.

6. Prevent developer mode:

From the Google Workspace Administration Console, in the menu on the left, we display the menu **Devices > Chrome > Settings and click on Users and browsers.**

Once on this screen, on the left side of the screen, <u>We will select the Organizational Unit on which we want to work</u>.

We look for the section called **User experience** and in the parameter **"Development tools"** we select **"Never allow the use of integrated development tools"**. To save the changes, we will click on the Save button that will appear at the top right of the screen:
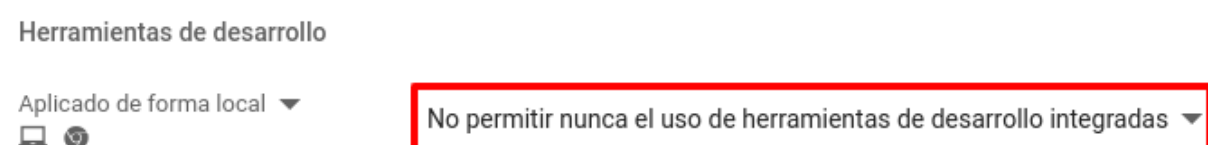
7. Disable the camera app to control camera use in Google Meet sessions:

From the Google Workspace Administration Console, we can disable both the camera resource at the Hardware level (it is completely disabled) or restrict the native camera application, but at the same time allow its use in Google Meet sessions and allow supervisors can control it from IMTLazarus with the "Google Meet - Inside!" functionality.

To restrict the camera from the Console, we will need to know the camera app ID. From the Chrome Web Store we find it at the following URL:

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

We are left with the final part of the ID: **hfhhnacclhffhdffklopdkcgdhifgngh**

From the Google Workspace Administration Console, in the menu on the left, we display the menu **Devices > Chrome > Apps and extensions > Users and browsers.** We select the **Organizational Unit** where we want to apply the restriction.
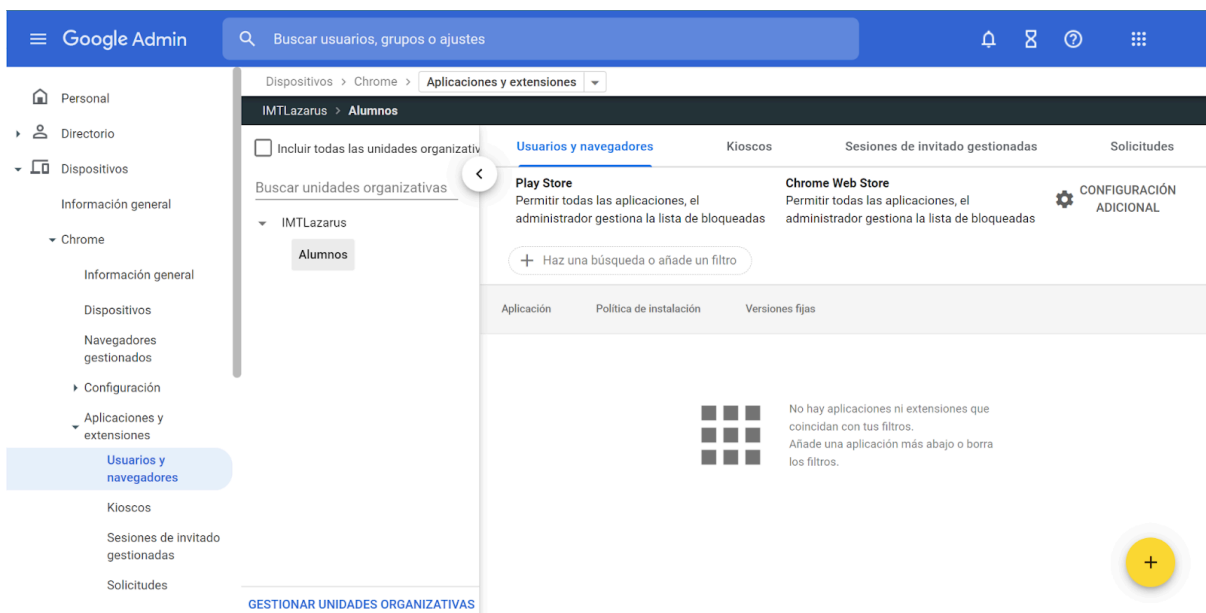
We click on the **Yellow + button > Add Chrome app or extension by ID**

In the window that opens, we enter the ID of the camera application that we obtained previously: **hfhhnacclhffhdffklopdkcgdhifgngh** and we press **KEEP**

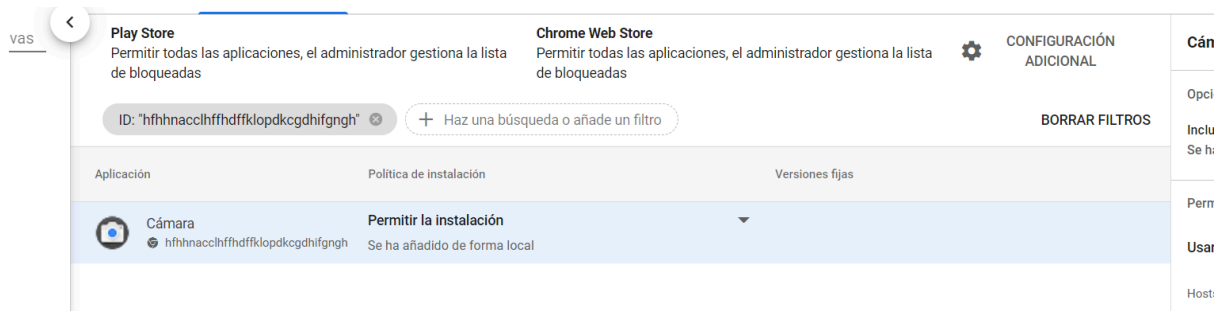**Añadir aplicación o extensión de Chrome por ID**

También puedes añadir aplicaciones y extensiones de Chrome especificando su ID. Si están fuera de Chrome Web Store, debes indicar también la URL donde se alojan.
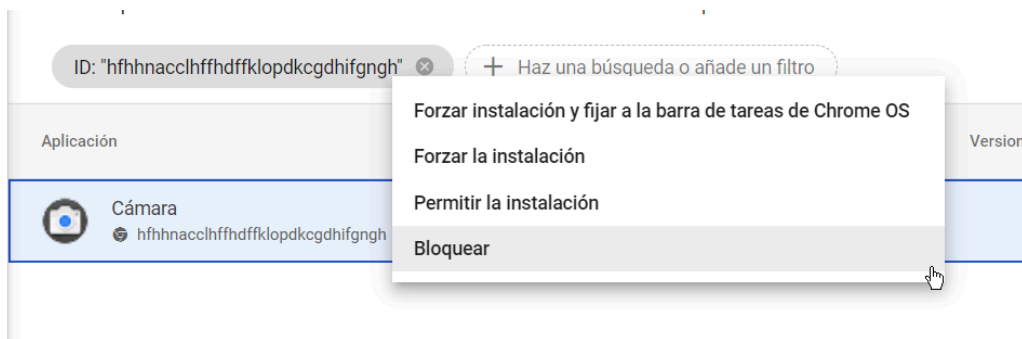
ID de extensión

hfhhnacclhffhdffklopdkcgdhifgngh

Desde Chrome Web Store ▼

CANCELAR   GUARDAR

Once added:

We click on the drop-down menu and select **"Block"**

And finally we press **KEEP** at the top right of the screen.
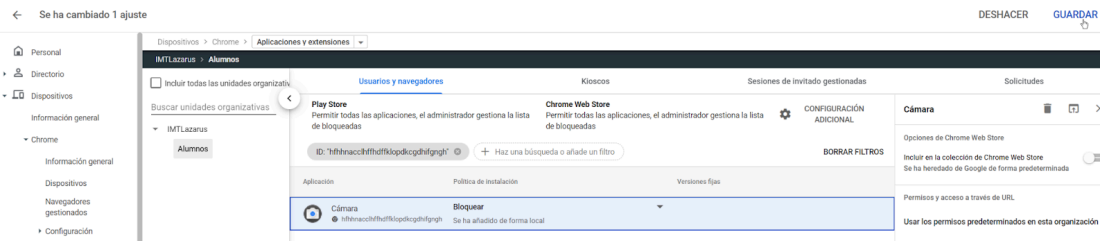
8. Disable javascript execution in the browser bar:

To prevent students from using javascript expressions to try to bypass the block, we must add an additional configuration.

From the Google Workspace Administration Console, in the menu on the left, we display the menu **Devices > Chrome > Settings and click on Users and browsers.** We select the **Organizational Unit** where we want to apply the restriction.

In **URL blocking** we add **javascript://*** and we press **KEEP** on top.

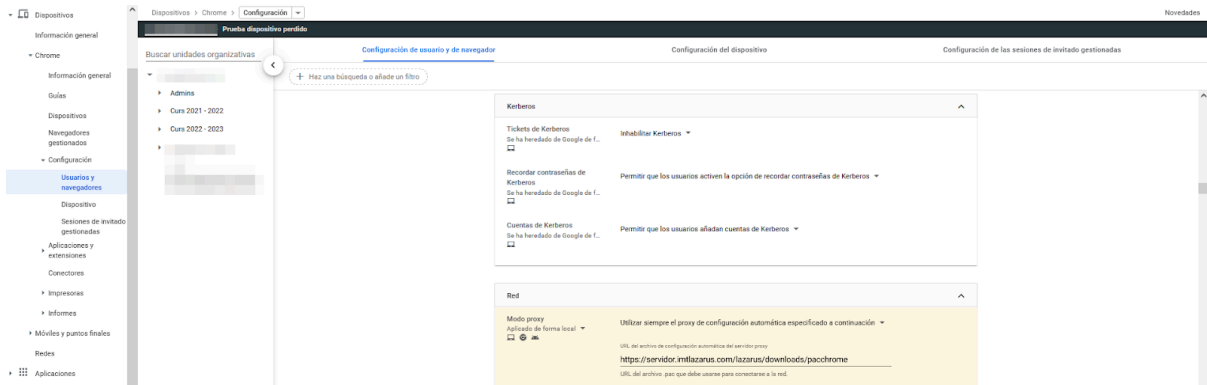# 9. PAC for security in access to the Play Store:

To guarantee the security of devices when accessing the Play Store, we must configure the following parameter from the Console:

From the Google Workspace Administration Console, in the menu on the left, we display the menu **Devices > Chrome > Settings and click on Users and browsers.** We select the **Organizational Unit** where we want to apply the restriction.

In the section of **Red**, within the parameter **"Modo proxy"** we select the option **"Always use the auto-configure proxy specified below":**
and we add the following URL: https://server.imtlazarus.com/lazarus/downloads/pacchrome

And finally we press **KEEP** at the top right of the screen.