

# IMTLazarus extension load on Google Workspace and security measures

## Index

Introducción	2
1. Instalación de la extensión IMTLazarus:	2
2. Impedir iniciar sesión con otras cuentas fuera del dominio y modo incógnito:	6
3. Impedir que los usuarios finalicen procesos con el administrador de tareas de Chrome:	8
4. Permisos de registro de los equipos:	9
5. Impedir iniciar sesión como invitado:	10
6. Impedir modo desarrollador:	10

**(N. del T. no se puede modificar el contenido del Índice, Los textos a incorporar son:)**

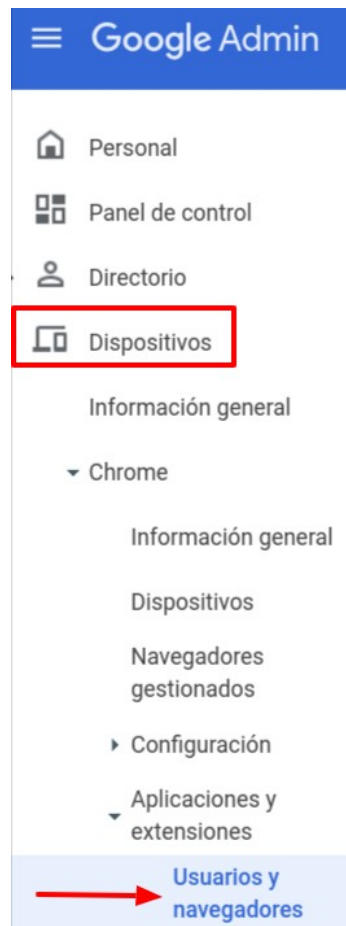
Introduction	2
1. Installation of the IMTLazarus extension:	2
2. Prevent logging in with other accounts outside the domain and incognito mode:	6
3. Prevent users from completing processes with Chrome task manager:	8
4. Equipment registration permits:	9
5. Prevent login as a guest:	10
6. Prevent developer mode:	10

## Introduction

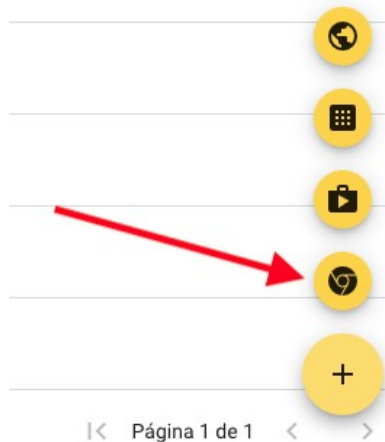
For IMTLazarus to work properly on Chrome devices, IMTLazarus recommends performing the following actions within the [Google Workspace Management Console](#). The first point is mandatory for IMTLazarus to work; the following are recommended so that users cannot skip filtering:

### 1. Installation of the IMTLazarus extension:

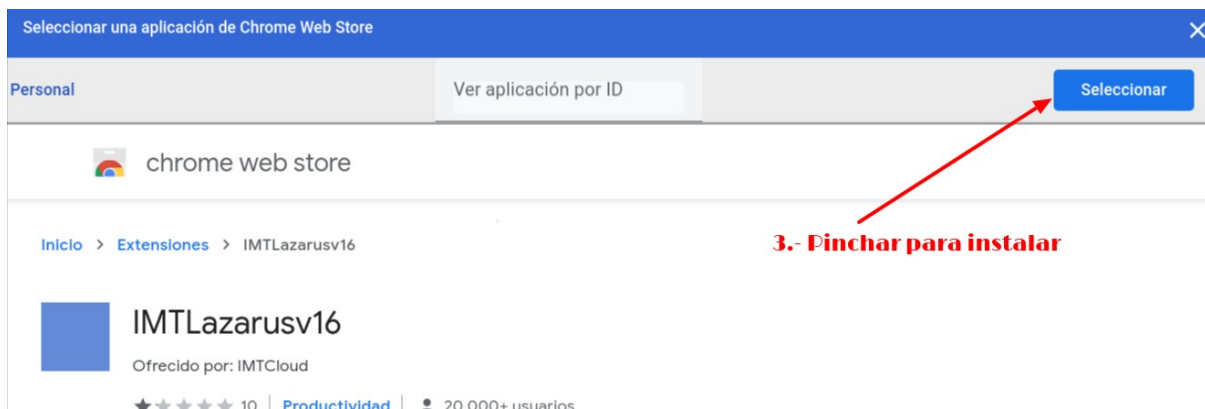
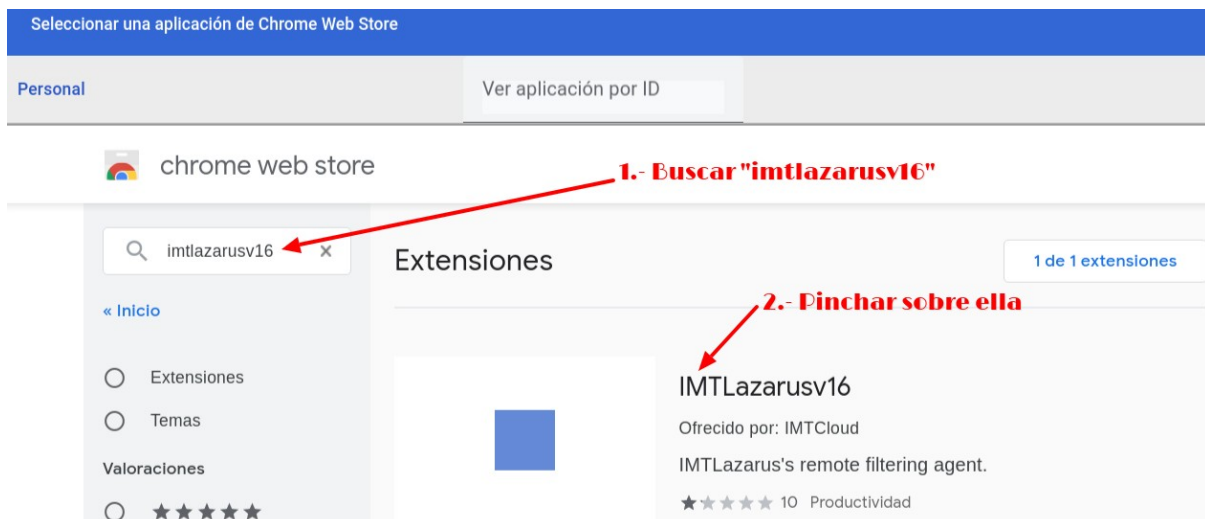
From the Google Workspace Management Console, in the menu on the left, we display the menu **Devices > Chrome > Chrome Devices Apps and Extensions** and click on **Users and browsers**:



Once on this screen, in the left part of the screen, we will select the Organizational Unit on which we want to work and, within the tab USERS AND BROWSERS, we will give the button "+" yellow we'll find down to the right and then the Chrome icon:



This will make us open a new window called "Select a Chrome Web Store App" from which we will have to look for the extension "IMTLazarusv9", click on it and then on the **blue button "Select"**:



Once the extension is available, we will verify that we have selected the correct Organizational Unit and select as Installation Policy "**Force Installation**" and hit the "**SAVE**"

button that will appear at the top right of the screen.

Usoarios y navegadores      Kioscos      Sesiones de invitado gestionada:

**Chrome Web Store**  
Permitir todas las aplicaciones, el administrador gestiona la lista de bloqueadas

CONFIGURACIÓN ADICIONAL

IMTLazarusv16

Opciones de Chrome

Incluir en la colección  
Se ha heredado de G

ID: "cgigopjakkeclhggchgnhmpmhghcbnaf" ✕      + Haz una búsqueda o añade un filtro

BORRAR FILTROS

Aplicación

IMTLazarusv16  
cgigopjakkeclhggchgnhmpmhghcbnaf

Forzar instalación y fijar a la barra de herramientas del navegador

Forzar la instalación

Permitir la instalación

Bloquear

If you have an older version of the IMTLazarus extension installed, remove it from this screen:

DESHACER 2      **GUARDAR**

> Aplicaciones y extensiones      NOVEDADES

USUARIOS Y NAVEGADORES      KIOSCOS      SESIONES DE INVITADO GESTIONADAS

ID: "oobadmchbbcmfpidofaknfhagomfdbkj" ✕      + Haz una búsqueda o añade un filtro      BORRAR FILTROS

Aplicación      Política de instalación

Permitir que los usuarios instalen otras aplicaciones y extensiones      Bloquear todas las demás aplicaciones y extensiones  
Se ha heredado de DominioGSuiteCentro.com

IMTLazarusv4      Forzar la instalación y fijar  
Se ha añadido de forma local

Opciones de Chrome Web Store

Incluir en la colección de Chrome Web Store  
Se ha heredado de Google de forma predeterminada

Permisos y acceso a través de URL

Usar los permisos predeterminados en esta organización

Hosts bloqueados

Una por línea

Hosts permitidos

Una por línea, los hosts permitidos anulan los bloqueados

Se ha heredado de Google de forma predeterminada

Filas por página: 10      < Página 1 de 1 >

Without leaving that screen, click on the wheel "Additional Configuration":

The screenshot shows the Chrome Web Store interface. At the top, there are tabs for 'Usuarios y navegadores', 'Kioscos', 'Sesiones de invitado gestionadas', and 'Solicitudes'. Below the tabs, there is a section for 'Chrome Web Store' with the text 'Permitir todas las aplicaciones, el administrador gestiona la lista de bloqueadas'. A red arrow points to a gear icon labeled 'CONFIGURACIÓN ADICIONAL' which is enclosed in a red box. Below this, there is a search bar with the ID 'cgigopjakkeclhggchgnhmpmhgcbnaf' and a search button. At the bottom, there is a table with columns 'Aplicación', 'Política de instalación', and 'Versiones fijas'. The first row shows 'IMTLazarusv16' with the policy 'Permitir la instalación' and the note 'Se ha añadido de forma local'.

Within the "Additional Application Configuration" section, under "Permissions and URLs", we check that the following parameters are NOT blocked:

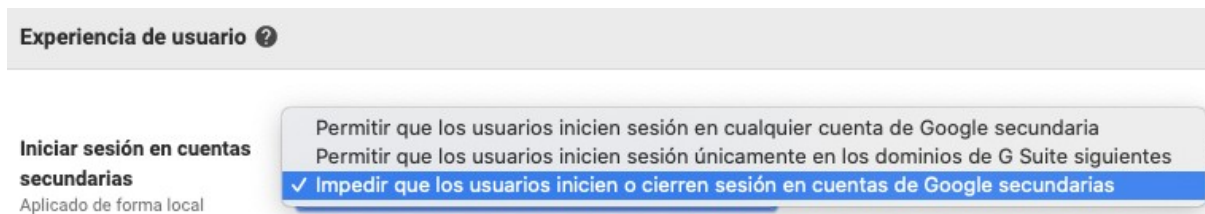
The screenshot shows the 'Permisos y URLs' section in the Chrome Web Store configuration. The text 'Se ha heredado de gtrainerdem...' is visible. A red text overlay says 'NO seleccionar estas opciones'. The permissions are listed in a grid format, each with an unchecked checkbox. The permissions are: 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 video, Proveedor de VPN, Solicitudes web, and Bloquear solicitudes web. The checkboxes for 'Captura de escritorio', 'Solicitudes web', and 'Bloquear solicitudes web' are highlighted with red boxes.

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

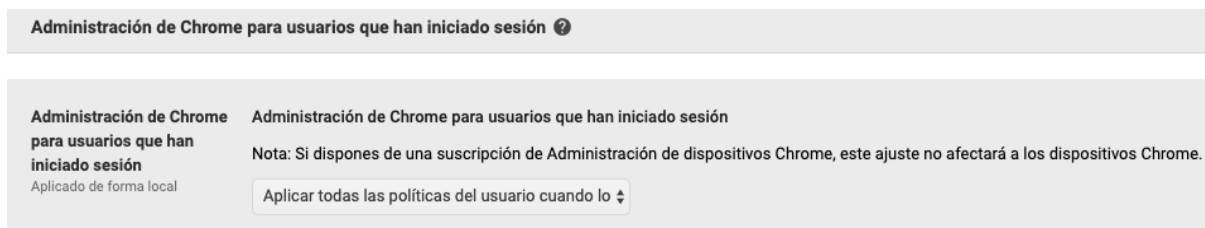
From the Google Workspace Management Console, in the menu on the left, drop down the menu **Devices > Chrome > Settings** and click on **Users and browsers**.

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

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




Without leaving that screen, in the "**Managing Chrome for Logged-in Users**" section, within **Managing Chrome for Logged-in Users** we'll select the option "**Apply all user policies when users log in to Chrome and provide a managed Chrome experience**".



In the "**Security**" section and in **Inactivity settings**, under "**Lock screen when suspended**" 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 click the "**SAVE**" button 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 **User Experience** section and in **Access by multiple login** we will select the option "**Block access by means of multiple login for this organization's user**" and we will click the "**SAVE**" button 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 completing processes with the Chrome task manager:

Without leaving the USER AND BROWSER SETTINGS tab, we will go to the **Applications and Extensions** section and in **Task Manager** we will select the option "**Prevent users from completing processes with the Chrome Task Manager**" and we will click the

“SAVE” button that will appear at the top right of the screen.

### Aplicaciones y extensiones

En la nueva [página de aplicaciones y extensiones](#) se centraliza todo el aprovisionamiento de aplicaciones y extensiones:

- Permitir y bloquear aplicaciones
- Forzar la instalación de aplicaciones
- Fijar aplicaciones a la barra de tareas
- Aplicaciones y extensiones recomendadas


La [página de configuración de aplicaciones](#) contiene ajustes adicionales para configurar las aplicaciones y extensiones:

- Tipos de aplicaciones permitidos
- Fuentes de instalación de aplicaciones y extensiones
- Permitir empaquetados de extensiones no seguros
- Bloquear extensiones según los permisos
- Hosts bloqueados en tiempo de ejecución
- Página principal de Chrome Web Store
- URL de la colección
- Aplicaciones privadas de la colección
- Permisos de Chrome Web Store
- Permitir que los usuarios publiquen aplicaciones alojadas privadas

Administrador de tareas  
Se ha heredado de gtrainerdem...  
🖥️

Permitir que los usuarios finalicen procesos con el administrador de tareas de Chrome

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





## 4. Equipment registration permits:

To prevent users from restoring the devices to the factory state and, therefore, uninstalling IMTLazarus and any other application, we need to enable mandatory computer registration, so that, if this happens (the reset or "powerwash" of the Chrome device), force you to enroll in the Administration Console to be able to use it.

To do this, in the Google Workspace Management 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 we want to work on.

Within this USER AND BROWSER SETTINGS tab, we will go to the **Registration Controls** section, configure the **Registration Permissions** setting as: **Do not allow users of this organization to register new or previously registered devices.**

We will hit the "Save" button that will appear at the top right of the screen.

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

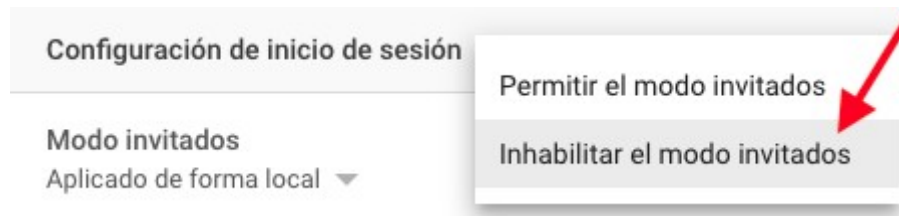
- **Obligation to re-register:** Force replay of device registration with user credentials when their data is deleted
- **Powerwash:** Do not allow Powerwash function to activate

We will hit the "Save" button that will appear at the top right of the screen.

This way, if a user resets the factory values, they will have to return the device to us so that we can re-register it manually with an Administrator account.

## 5. Prevent login as a guest:

From the same window, click on the DEVICE SETTINGS tab, go to the **Login Settings section** and in **Guest Mode** select the "**Disable Guest Mode**" option and hit the "**SAVE**" button which will appear at the top right of the screen.



If we have left the screen, we will be able to return to the main screen of the Administration Console and, in the menu on the left, we will display the menu **Devices > Chrome > Settings and click on Device**.

We will select the Organizational Unit where we want to apply the changes. We looked for the section called **Login Settings** and in the parameter "**Guest Mode**" we marked "**Disable Guest Mode**". To save the changes, we will click the **Save** button that will appear at the top right of the screen.

## 6. Prevent developer mode:

From the Google Workspace Management Console, in the menu on the left, drop down 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 we want to work on.

We look for the section called **User Experience** and in the parameter "**Development tools**" select "**Never allow the use of integrated development tools**". To save the changes, we will click the **Save** button that will appear at the top right of the screen:

Herramientas de desarrollo

Aplicado de forma local ▼



No permitir nunca el uso de herramientas de desarrollo integradas ▼