

# Chargement de l'extension IMTLazarus sur Google Workspace et mesures de sécurité

## Index

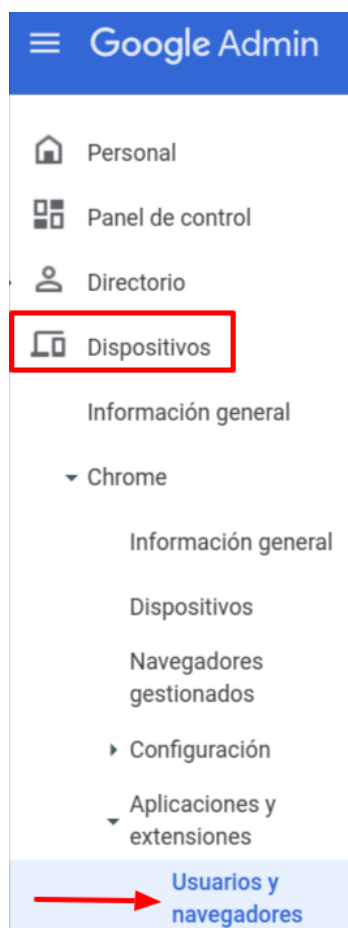
Introduction	2
1. Installation de l'extension IMTLazarus:	2
2. Empêcher la connexion avec d'autres comptes en dehors du domaine et du mode incognito:	6
3. Empêcher les utilisateurs de terminer les processus avec le gestionnaire de tâches Chrome:	8
4. Permis d'immatriculation d'équipement:	9
5. Empêcher l'ouverture de session en tant qu'invité:	10
6. Empêcher le mode développeur:	10
7. Désactiver l'app caméra pour contrôler l'utilisation de la caméra lors des sessions de Google Meet:	11
8. Désactiver l'exécution de javascript dans la barre du navigateur:	13
9. PAC sécurité lors de l'accès à Play Store:	13

## Introduction

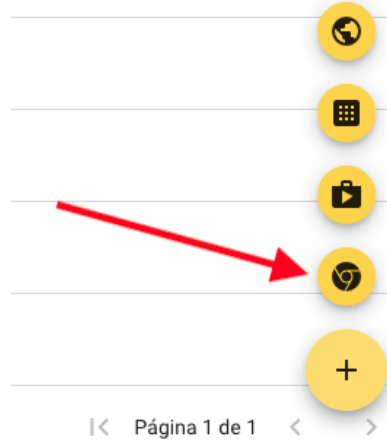
Pour que IMTLazarus fonctionne correctement sur les appareils Chrome, IMTLazarus recommande d'effectuer les actions suivantes dans la Console de Gestion de Google Workspace. Le premier point est obligatoire pour que IMTLazarus fonctionne ; les éléments suivants sont recommandés afin que les utilisateurs ne puissent pas sauter le filtrage :

### 1. Installation de l'extension IMTLazarus:

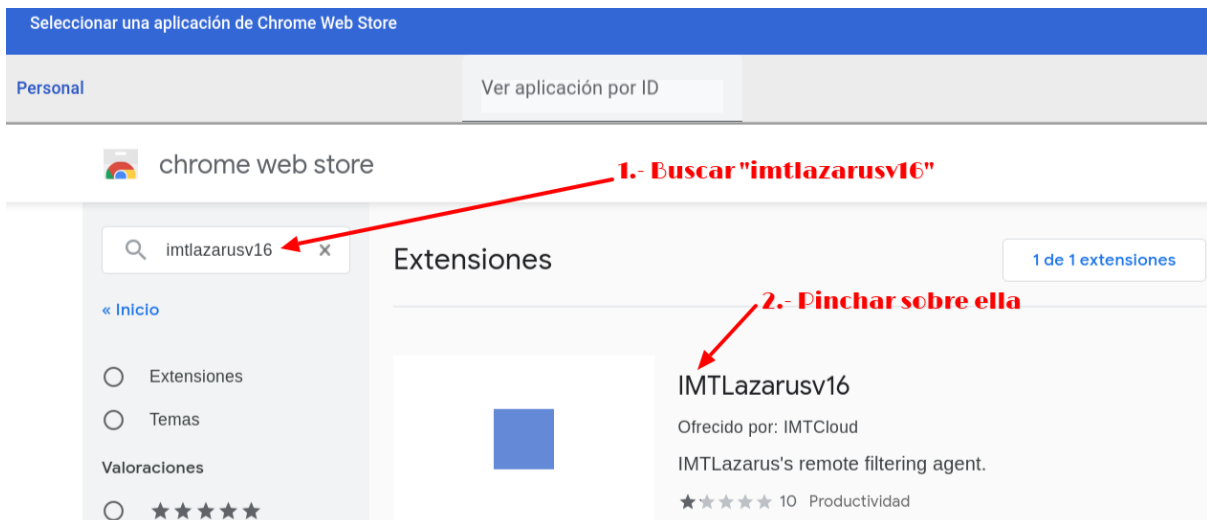
À partir de la console de gestion de l'espace de travail de Google, dans le menu à gauche, nous affichons le menu Appareils > Chrome > Applications et extensions Appareils Chrome et cliquez sur Utilisateurs et navigateurs:



Une fois sur cet écran, dans la partie gauche de l'écran, nous allons sélectionner l'unité organisationnelle sur laquelle nous voulons travailler et, dans l'onglet UTILISATEURS ET NAVIGATEURS, nous cliquons sur le bouton "+" jaune, nous allons trouver vers le bas à droite, puis l'icône Chrome:



Cela nous fera ouvrir une nouvelle fenêtre appelée "Sélectionnez un Chrome Web Store App" à partir de laquelle nous devons chercher l'extension "IMTLazarusv16", cliquez dessus et puis sur le bouton bleu "Sélectionner":



Une fois l'extension est disponible, nous vérifions que nous avons sélectionné la bonne unité organisationnelle et nous sélectionnons comme politique d'installation « Forcer l'installation » et nous cliquons sur le bouton « SAUVEGARDER » qui apparaîtra en haut à droite de l'écran.

**Usuarios y navegadores**      Kioscos      Sesiones de invitado gestionadas

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

CONFIGURACIÓN ADICIONAL

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

IMTLazarusv16  
Opciones de Chrome  
Incluir en la colección  
Se ha heredado de G

Si vous avez installé une ancienne version de l'extension IMTLazarus, supprimez-la de cet écran:

DESHACER 2      **GUARDAR**

> Aplicaciones y extensiones      NOVEDADES

USUARIOS Y NAVEGADORES      KIOSCOS      SESIONES DE INVITADO GESTIONADAS

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

IMTLazarusv4

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 >

Sans quitter cet écran, cliquez sur la roue "Additional Configuration":

Usuarios y navegadores      Kioscos      Sesiones de invitado gestionadas      Solicitudes

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

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

Aplicación	Política de instalación	Versiones fijas
IMTLazarusv16 cgigopjakkeclhggchgnhmpmhgcbnaf	Permitir la instalación Se ha añadido de forma local	

Dans la section "Configuration Complémentaire de l'Application", sous "Permissions et URL", nous vérifions que les paramètres suivants ne sont PAS bloqués:

**Permisos y URLs**  
Se ha heredado de [gtrainerdem...](#)

**NO seleccionar estas opciones**

Bloquear extensiones según los permisos

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

## 2. Empêcher la connexion avec d'autres comptes en dehors du domaine et du mode incognito:

À partir de la console de gestion de l'espace de travail de Google, dans le menu à gauche, descendez le menu **Appareils > Chrome > Paramètres** et cliquez sur **Utilisateurs et navigateurs**.

Une fois sur cet écran, à gauche de l'écran, nous sélectionnerons l'Unité Organisationnelle sur laquelle nous voulons travailler.

Dans cet onglet CONFIGURATION UTILISATEUR ET NAVIGATEUR, nous allons dans la section Expérience utilisateur et dans Ouvrir une session dans les comptes secondaires, nous devons cliquer et sélectionner l'option "Empêcher les utilisateurs de se connecter ou de se déconnecter des comptes Google secondaires". Pour appliquer les modifications, nous cliquerons sur le bouton « SAUVEGARDER » qui apparaîtra en haut à droite de l'écran.

Experiencia de usuario ?

**Iniciar sesión en cuentas secundarias**  
Aplicado de forma local

- Permitir que los usuarios inicien sesión en cualquier cuenta de Google secundaria
- Permitir que los usuarios inicien sesión únicamente en los dominios de G Suite siguientes
- Impedir que los usuarios inicien o cierren sesión en cuentas de Google secundarias

Sans quitter cet écran, dans la section "**Gestion de Chrome pour les utilisateurs connectés**", dans **Gestion de Chrome pour les utilisateurs connectés**, nous allons sélectionner l'option "**Appliquer toutes les politiques utilisateur lorsque les utilisateurs se connectent à Chrome et fournir une expérience Chrome gérée**".

Administración de Chrome para usuarios que han iniciado sesión ?

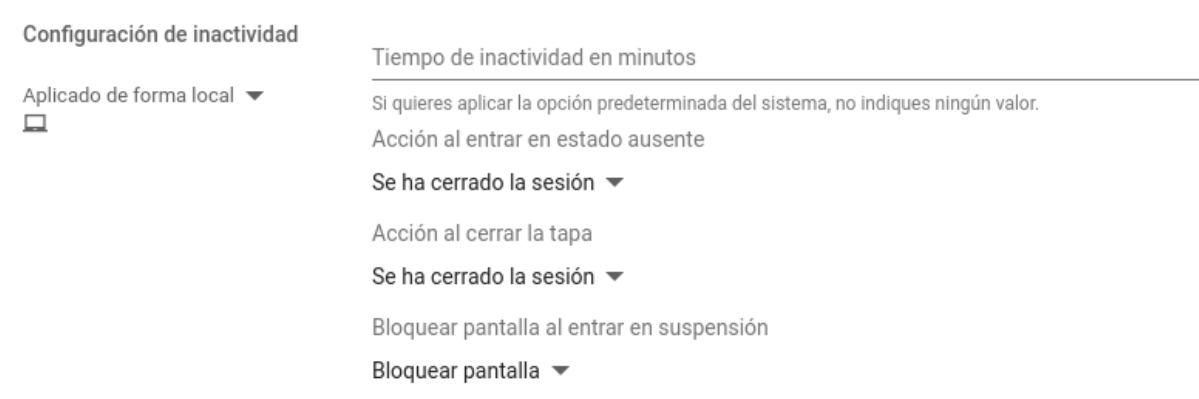
**Administración de Chrome para usuarios que han iniciado sesión**  
Aplicado de forma local

Administración de Chrome para usuarios que han iniciado sesión

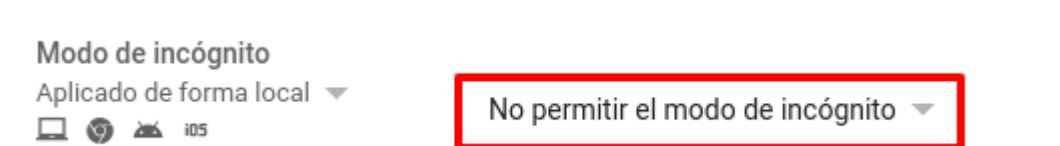
Nota: Si dispones de una suscripción de Administración de dispositivos Chrome, este ajuste no afectará a los dispositivos Chrome.

Aplicar todas las políticas del usuario cuando lo ↕

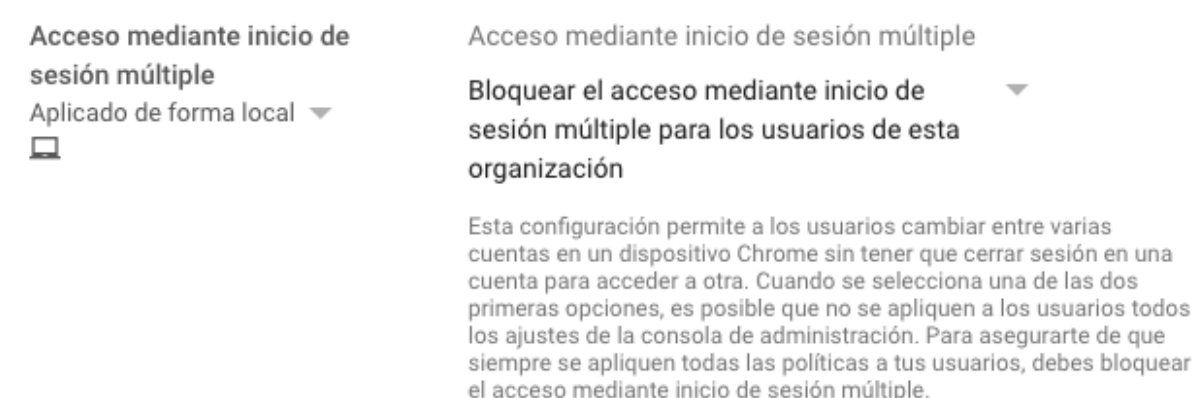
Dans la section "**Sécurité**" et dans **Paramètres d'inactivité**, sous "**Écran de verrouillage en cas de suspension**", nous sélectionnons l'option "Verrouiller l'Écran" :



Juste en dessous de ce paramètre et dans la même section Sécurité, en **Mode Incognito**, nous sélectionnerons l'option "**Ne pas autoriser le mode Incognito**" et nous cliquerons sur le bouton "SAUVEGARDER" qui apparaîtra en haut à droite de l'écran.



Sans laisser où nous en sommes dans l'onglet CONFIGURATION DE L'UTILISATEUR ET NAVIGATEUR, nous allons à la section **Expérience de l'Utilisateur** et dans **Accès par connexion multiple** nous allons sélectionner l'option "**Bloquer l'accès au moyen de plusieurs connexions pour l'utilisateur de cette organisation**" et nous allons cliquer sur le bouton "SAUVEGARDEE" qui apparaîtra en haut à droite de l'écran.



### 3. Empêcher les utilisateurs de terminer les processus avec le gestionnaire de tâches Chrome:

Sans quitter l'onglet CONFIGURATION DE L'UTILISATEUR ET NAVIGATEUR, nous allons à la section **Applications et Extensions** et dans le **Gestionnaire des tâches**, nous allons sélectionner l'option "**Empêcher les utilisateurs de terminer les processus avec le Gestionnaire des tâches Chrome**" et nous allons cliquer sur le bouton « SAUVEGARDER » qu'apparaîtra en haut à droite de l'écran.


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. Permis d'immatriculation d'équipement:

Pour empêcher les utilisateurs de restaurer les appareils à l'état d'usine et, par conséquent, désinstaller IMTLazarus et toute autre application, nous devons activer l'enregistrement obligatoire de l'ordinateur, de sorte que, si cela se produit (la réinitialisation ou "powerwash" de l'appareil Chrome), vous oblige à vous inscrire à la console d'administration pour pouvoir l'utiliser.

Pour ce faire, dans le Google Workspace Management Console, dans le menu à gauche, nous affichons le menu **Appareils > Chrome > Paramètres et cliquez sur Utilisateurs et navigateurs**.

Une fois sur cet écran, à gauche de l'écran, nous sélectionnerons l'Unité Organisationnelle sur laquelle nous voulons travailler

Dans cet onglet CONFIGURATION DE L'UTILISATEUR ET NAVIGATEUR, nous allons dans la section Contrôles d'enregistrement, configurer le paramètre Autorisations d'enregistrement comme suit : **Ne pas permettre aux utilisateurs de cette organisation d'enregistrer des appareils neufs ou déjà enregistrés**.

Nous allons appuyer sur le bouton "SAUVEGARDER" qui apparaîtra en haut à droite de l'écran.

Sans quitter l'endroit où nous sommes, dans l'onglet CONFIGURATION DES APPAREILS, nous allons à la section Enregistrement et accès et marquons ce qui suit :

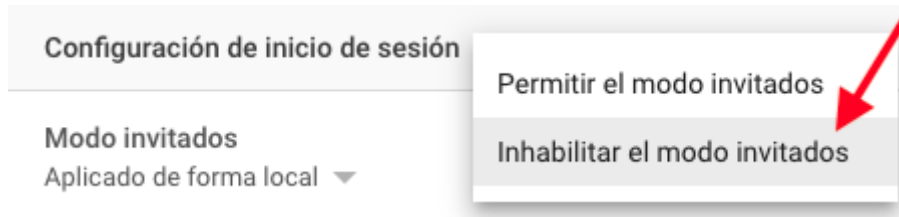
- **Obligation de réinscrire** l'enregistrement : forcer la relecture de l'enregistrement de l'appareil avec les identifiants de l'utilisateur lorsque ses données sont supprimées
- **Powerwash:** ne pas activer la fonction Powerwash

Nous allons appuyer sur le bouton "SAUVEGARDER" qui apparaîtra en haut à droite de l'écran.

De cette façon, si un utilisateur réinitialise les valeurs d'usine, il devra nous retourner l'appareil afin que nous puissions l'enregistrer à nouveau manuellement avec un compte administrateur.

## 5. Empêcher l'ouverture de session en tant qu'invité:

Dans la même fenêtre, cliquez sur l'onglet CONFIGURATION DES APPAREILS, accédez à la section **Paramètres de connexion** et en **Mode Invité** sélectionnez l'option "**Désactiver le mode invité**" et cliquez sur le bouton "SAUVEGARDER" qui apparaîtra en haut à droite de l'écran.



Si nous avons quitté l'écran, nous serons en mesure de revenir à l'écran principal de la console d'administration et, dans le menu à gauche, nous allons afficher le menu **Appareils > Chrome > Paramètres** et cliquez sur **Appareil**.

Nous sélectionnerons l'Unité Organisationnelle où nous voulons appliquer les changements. Nous cherchons la section appelée **Paramètres de connexion** et dans le paramètre "**Mode invité**" nous avons marqué "**Désactiver le mode invité**". Pour enregistrer les modifications, nous cliquerons sur le bouton SAUVEGARDER qui apparaîtra en haut à droite de l'écran.

## 6. Empêcher le mode développeur:

À partir de la console de gestion de l'espace de travail de Google, dans le menu à gauche, descendez le menu **Appareils > Chrome > Paramètres** et cliquez sur **Utilisateurs et navigateurs**.

Une fois sur cet écran, à gauche de l'écran, nous sélectionnerons l'Unité Organisationnelle sur laquelle nous voulons travailler.

Nous recherchons la section appelée **Expérience utilisateur** et dans le paramètre "**Outils de développement**" sélectionnez "**Ne jamais autoriser l'utilisation d'outils de développement intégrés**". Pour enregistrer les modifications, nous cliquerons sur le bouton SAUVEGARDER qui apparaîtra en haut à droite de l'écran:

Herramientas de desarrollo

Aplicado de forma local ▾



No permitir nunca el uso de herramientas de desarrollo integradas ▾

## 7. Désactiver l'app caméra pour contrôler l'utilisation de la caméra lors des sessions de Google Meet:

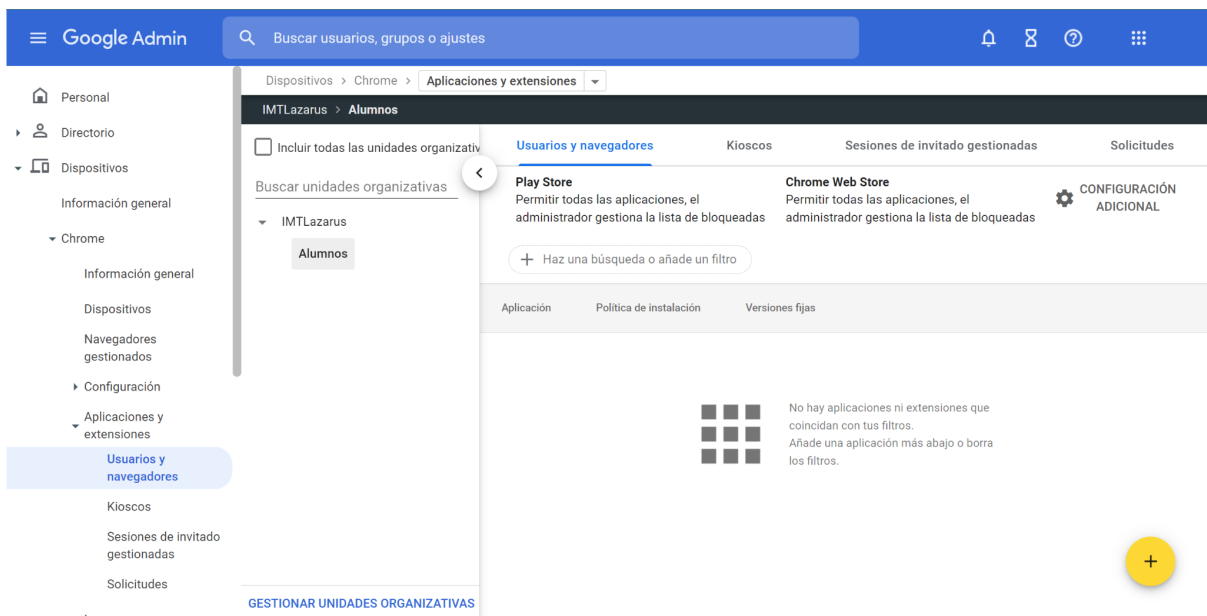
Depuis la console de gestion de Google Workspace, nous pouvons désactiver à la fois la ressource de l'appareil photo au niveau matériel (complètement désactivé) ou restreindre l'application native de l'appareil photo, mais à son tour permettre son utilisation dans les sessions de Google Meet et permettre aux superviseurs de le contrôler à partir d'IMTLazarus avec la fonctionnalité "Google Meet - Inside!".

Pour restreindre l'appareil photo depuis la console, nous devons connaître l'identifiant de l'application de l'appareil photo. Depuis le Chrome Web Store, nous la localisons sur l'URL suivante:

<https://chrome.google.com/webstore/detail/camera/hfhhnacclhffhdffklopdkcgdhifgngh>

Nous gardons la dernière partie de l'ID: **hfhhnacclhffhdffklopdkcgdhifgngh**

Depuis la console d'administration de Google Workspace, dans le menu de gauche, nous affichons le menu **Appareils > Chrome > Applications et extensions > Utilisateurs et navigateurs**. Nous choisissons l'**Unité Organisationnelle** où nous voulons appliquer la restriction.



Cliquez sur le **Bouton + jaune > Ajouter l'application ou l'extension Chrome par ID**



Dans la fenêtre qui s'ouvre, nous saisissons l'ID de l'application de la caméra que nous avons obtenue précédemment: **hfhhnacclhffhdfklopdkcgdhifgngh** et nous cliquons sur **ENREGISTRER**

**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

Desde Chrome Web Store ▼

CANCELAR GUARDAR

Après avoir ajouté:

The screenshot shows the Chrome management interface. At the top, there are tabs for 'Play Store', 'Chrome Web Store', and 'CONFIGURACIÓN ADICIONAL'. Below the tabs, there is a search bar with the ID 'hfhhnacclhffhdfklopdkcgdhifgngh' and a filter button. A table lists the installed applications. The 'Cámara' application is highlighted, showing its policy as 'Permitir la instalación' and a note 'Se ha añadido de forma local'.

Aplicación	Política de instalación	Versiones fijas
Cámara hfhhnacclhffhdfklopdkcgdhifgngh	Permitir la instalación Se ha añadido de forma local	

Cliquez sur la liste déroulante et sélectionnez **"Bloquer"**

This image is a close-up of the application list from the previous screenshot. The 'Cámara' application is selected, and a dropdown menu is open, showing the following options: 'Forzar instalación y fijar a la barra de tareas de Chrome OS', 'Forzar la instalación', 'Permitir la instalación', and 'Bloquear'. The 'Bloquear' option is highlighted by the mouse cursor.

Enfin, nous cliquons sur **ENREGISTRER** en haut à droite de l'écran.

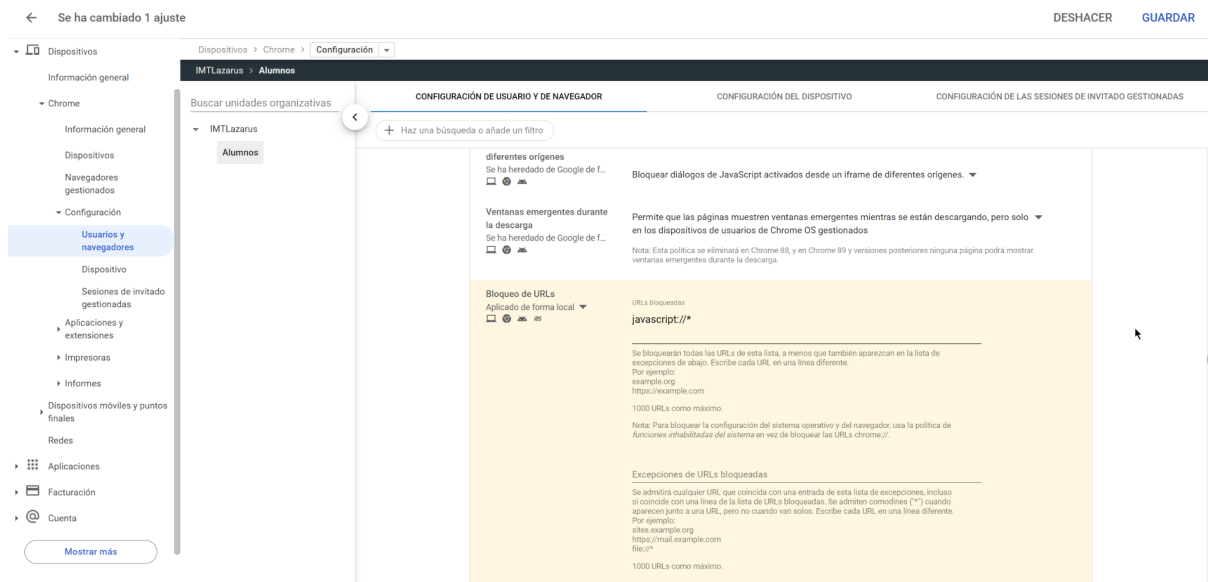
The screenshot shows the full Chrome management interface. The 'Cámara' application is now listed with a policy of 'Bloquear'. In the top right corner, the 'ENREGISTRAR' button is highlighted with a mouse cursor.

## 8. Désactiver l'exécution de javascript dans la barre du navigateur:

Pour empêcher les élèves d'utiliser des expressions javascript pour contourner le verrouillage, nous devons ajouter des paramètres supplémentaires.

Depuis la console d'administration de Google Workspace, dans le menu de gauche, nous affichons le menu **Appareils > Chrome > Paramètres** et nous cliquons sur **Utilisateurs et navigateurs**. Nous choisissons l'**Unité Organisationnelle** où nous voulons appliquer la restriction.

Dans **Verrouillage URLs**, nous ajoutons **javascript://\*** et nous cliquons sur **ENREGISTRER** en haut.



## 9. PAC sécurité lors de l'accès à Play Store:

Pour assurer la sécurité des périphériques lors de l'accès au Play Store, nous devons configurer le paramètre suivant dans la console d'administration :

À partir de la console de gestion Google Workspace, dans le menu de gauche, faites défiler le menu **Appareils > Chrome > Paramètres** et cliquez sur **Utilisateurs et navigateurs**. Nous choisissons l'unité organisationnelle où nous voulons appliquer la restriction.

Dans la section "Network", à l'intérieur du paramètre "Mode mandataire", sélectionnez le menu déroulant pour choisir l'option "Toujours utiliser la configuration automatique du mandataire indiquée ci-dessous" et ajoutez l'URL suivante :

<https://server.imtlazarus.com/lazarus/downloads/pacchrome>

← 1 setting changed REVERT **SAVE**

Devices > Chrome > Settings What's new?

**User & browser settings** Device settings

+ Search or add a filter

**Network**

Proxy mode <sup>ⓘ</sup>  
Locally applied <sup>⌵</sup>  
Always use the proxy auto-config specified below <sup>?</sup>

Proxy server auto configuration file URL  
<https://server.imtlazarus.com/lazarus/downloads/pacchrome>  
URL of the .pac file that should be used for network connections.

Ignore proxy on captive portals  
Inherited from Google default <sup>⌵</sup>

Keep policies for captive portal pages <sup>⌵</sup>

Supported authentication schemes  
Inherited from Google default <sup>⌵</sup>

Supported authentication schemes  
 Basic  Digest  NTLM  
 Negotiate

Specifies which HTTP authentication schemes are supported by Google Chrome. The default uses all four schemes.

Left sidebar: Home, Dashboard, Directory, Devices (Overview, Chrome (Overview, Guides, Devices, Managed browsers), Settings (Users & browsers (selected), Device, Managed guest sessions), Apps & extensions, Connectors)

Enfin, nous cliquons sur **ENREGISTRER** en haut à droite de l'écran.