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

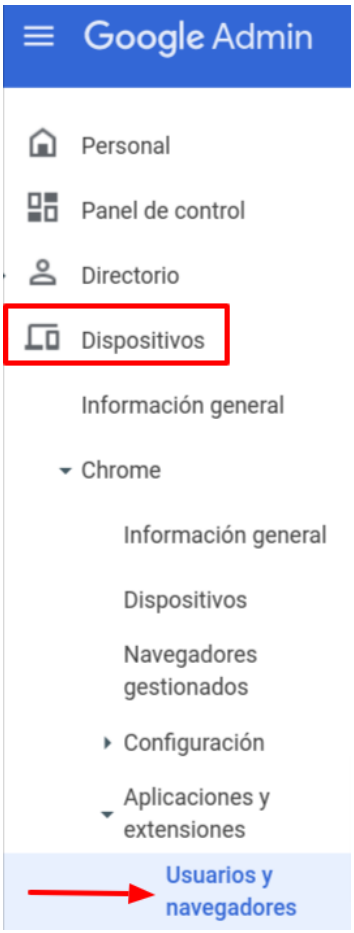
Index

Introduction

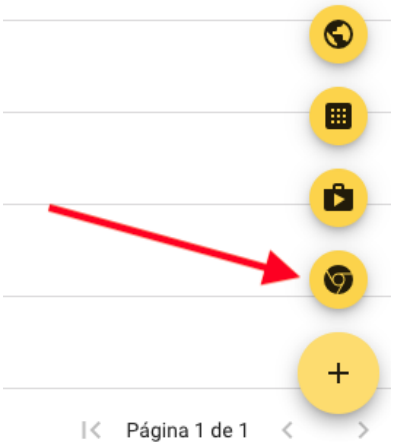
Pour que IMTLazarus fonctionne correctement sur les appareils Chrome, IMTLazarus recommande d'effectuer les actions suivantes dans la Console de Gestion de Google Workspace. Le premier point est obligatoire pour que IMTLazarus fonctionne ; les éléments suivants sont recommandés afin que les utilisateurs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

1. Installation de l'extension IMTLazarus:

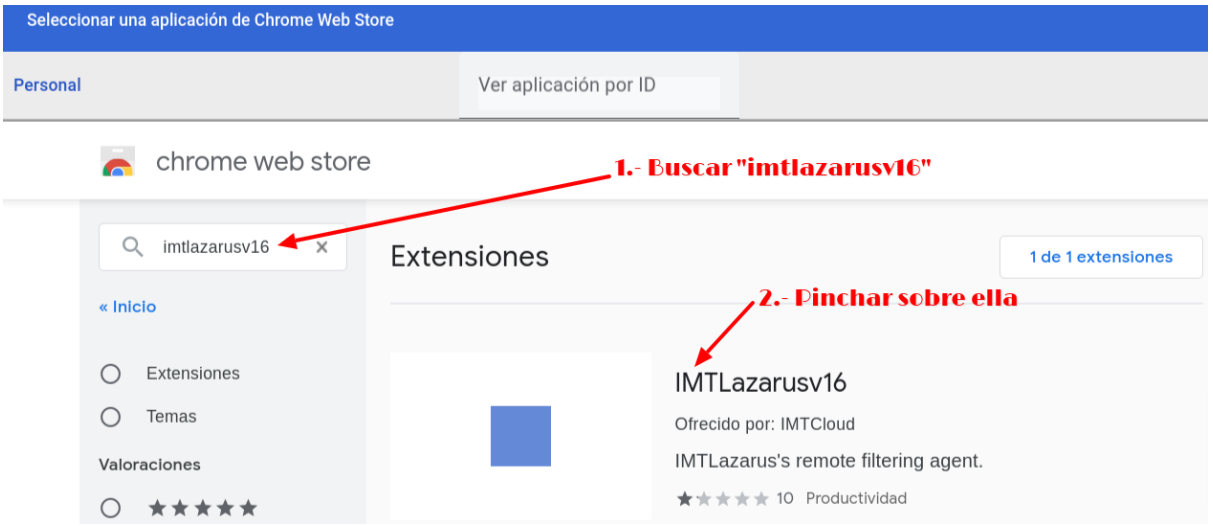
À partir de la console de gestion de l'espace de travail de Google, dans le menu à gauche, nous affichons le menu Appareils > Chrome > Applications et extensions Appareils Chrome et cliquez sur Utilisateurs et navigateurs:



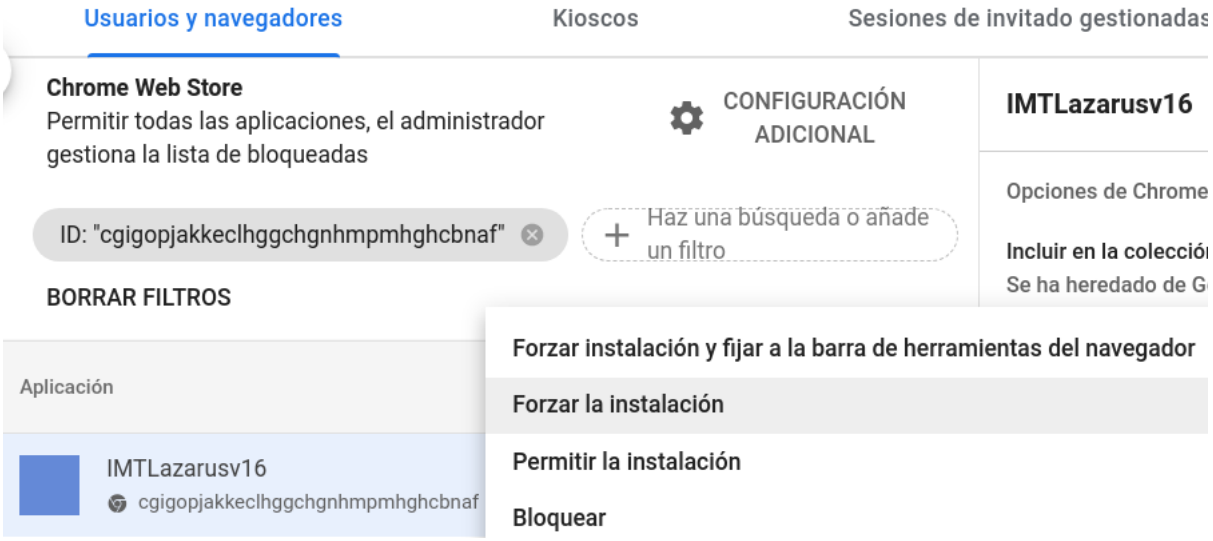
Une fois sur cet écran, dans la partie gauche de l'écran, nous allons sélectionner l'unité organisationnelle sur laquelle nous voulons travailler et, dans l'onglet UTILISATEURS ET NAVIGATEURS, nous cliqons sur le bouton "+" jaune, nous allons trouver vers le bas à droite, puis l'icône Chrome:



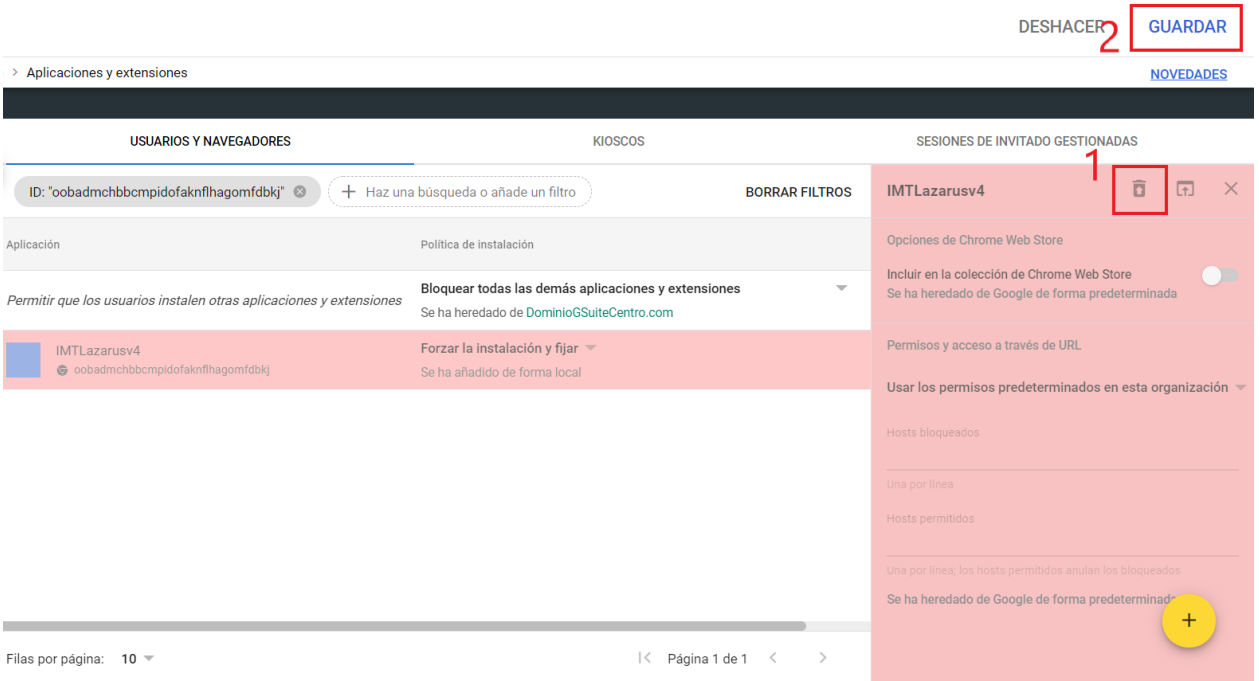
Cela nous fera ouvrir une nouvelle fenêtre appelée "Sélectionnez un Chrome Web Store App" à partir de laquelle nous devrons chercher l'extension "IMTLazarusv16", cliquez dessus et puis sur le bouton bleu "Sélectionner":



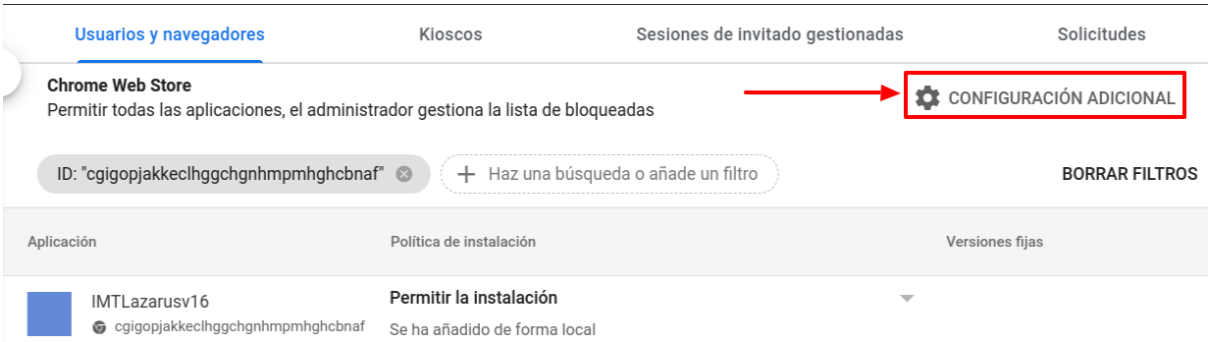
Une fois l'extension est disponible, nous vérifierons que nous avons sélectionné la bonne unité organisationnelle et nous sélectionnons comme politique d'installation « Forcer l'installation » et nous clickons sur le bouton « SAUVEGARDER » qui apparaîtra en haut à droite de l'écran.



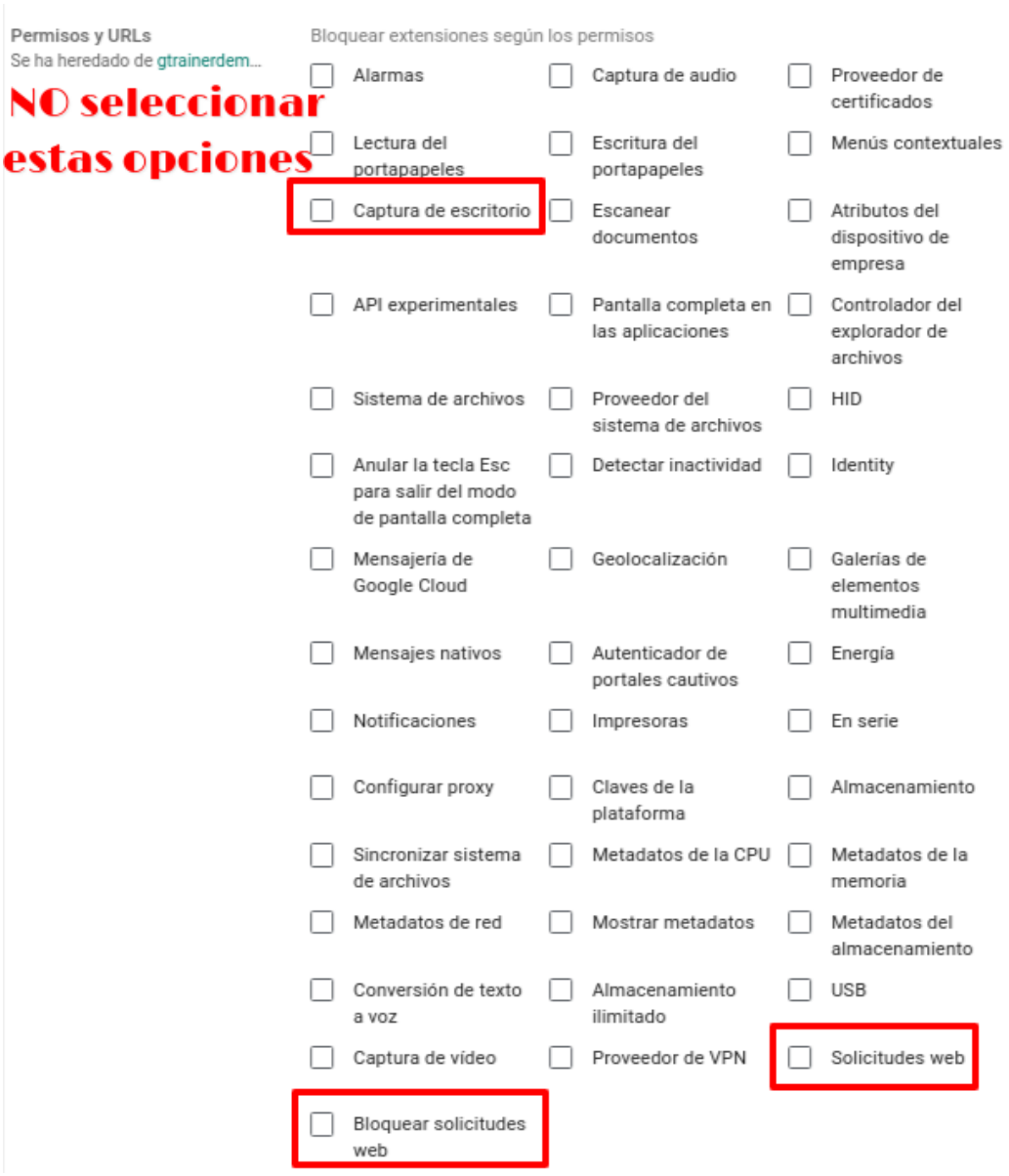
Si vous avez installé une ancienne version de l'extension IMTLazarus, supprimez-la de cet écran:



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



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

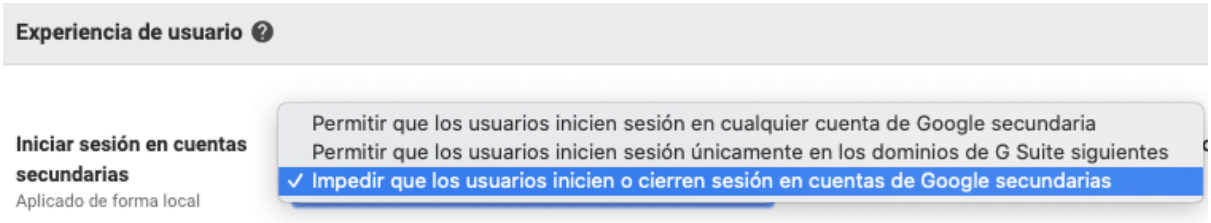


2. Empêcher la connexion avec d'autres comptes en dehors du domaine et du mode incognito:

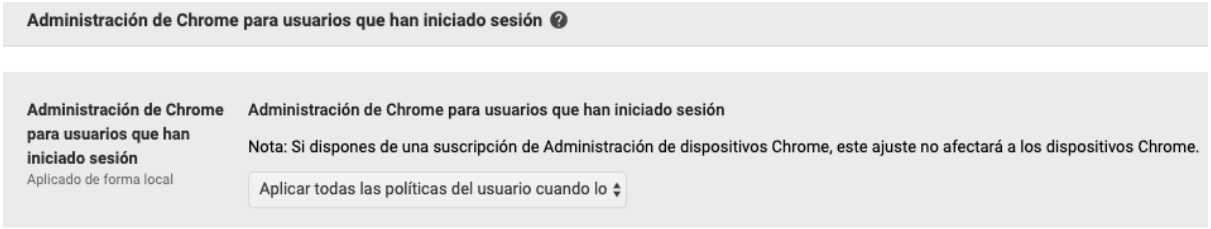
À partir de la console de gestion de l'espace de travail de Google, dans le menu à gauche, descendez le menu **Appareils > Chrome > Paramètres et cliquez sur Utilisateurs et navigateurs**.

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

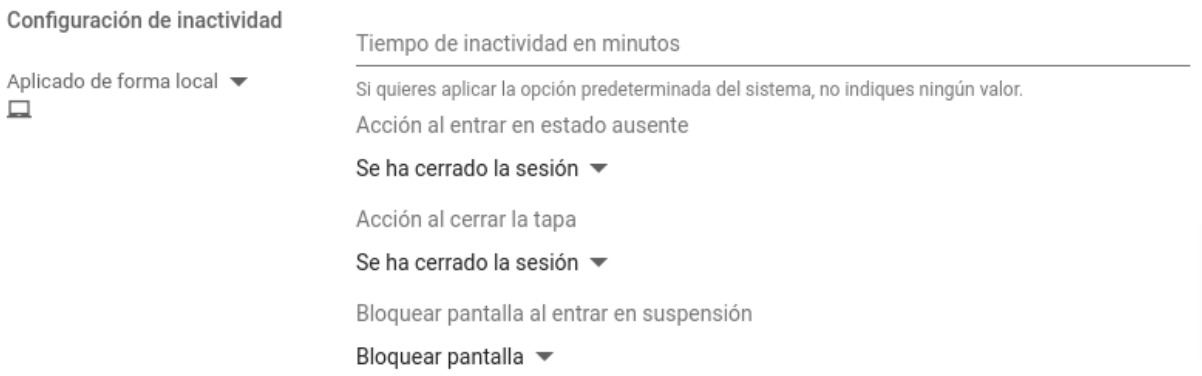
Dans cet onglet CONFIGURATION UTILISATEUR ET NAVIGATEUR, nous allons dans la section Expérience utilisateur et dans Ouvrir une session dans les comptes secondaires, nous devrons cliquer et sélectionner l'option "Empêcher les utilisateurs de se connecter ou de se déconnecter des comptes Google secondaires".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



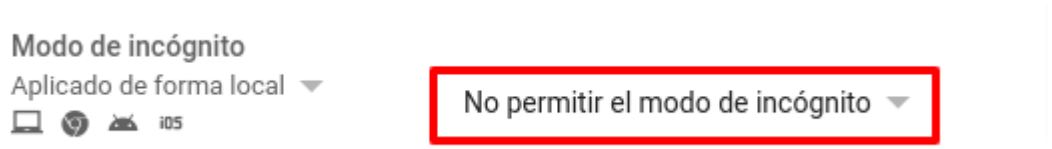
Sans quitter cet écran, dans la section "**Gestion de Chrome pour les utilisateurs connectés**", dans **Gestion de Chrome pour les utilisateurs connectés**, nous allons sélectionner l'option "**Appliquer toutes les politiques utilisateur lorsque les utilisateurs se connectent à Chrome et fournir une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



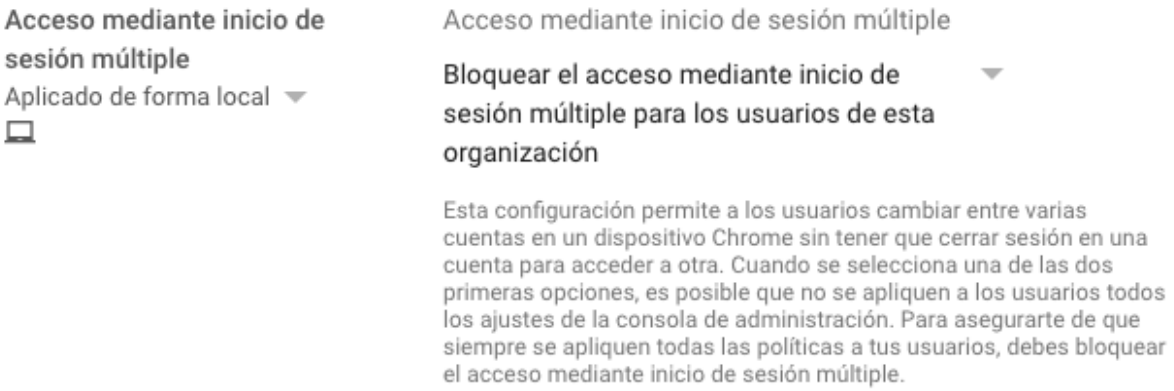
Dans la section "**Sécurité**" et dans **Paramètres d'inactivité**, sous "**Écran de verrouillage en cas de suspension**", nous sélectionnons l'option "Verrouiller l'Écran" :



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.

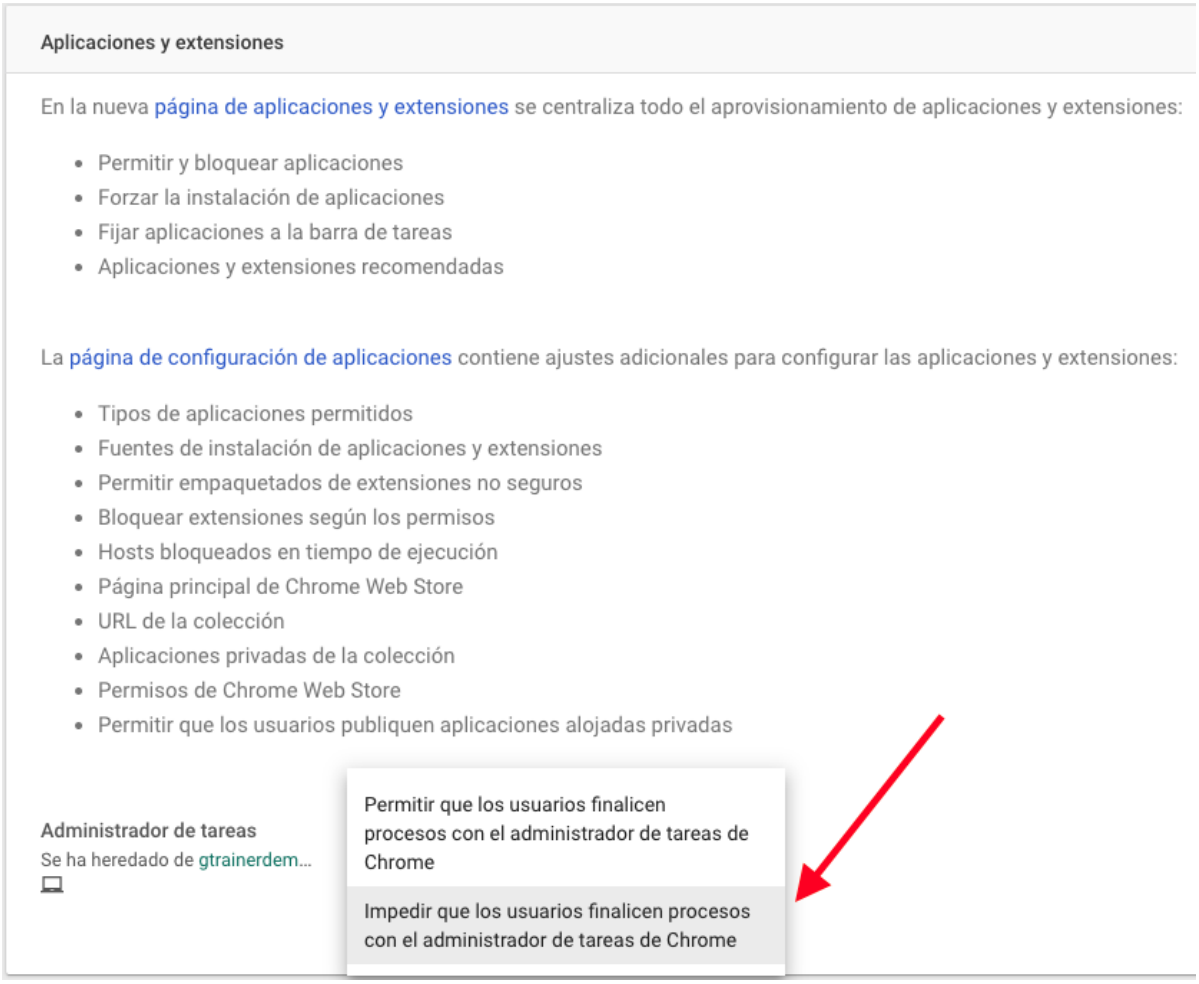


Sans laisser où nous en sommes dans l'onglet CONFIGURATION DE L'UTILISATEUR ET NAVIGATEUR, nous allons à la section **Expérience de l'Utilisateur** et dans **Accès par connexion multiple** nous allons sélectionner l'option "**Bloquer l'accès au moyen de plusieurs connexions pour l'utilisateur de cette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



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 :

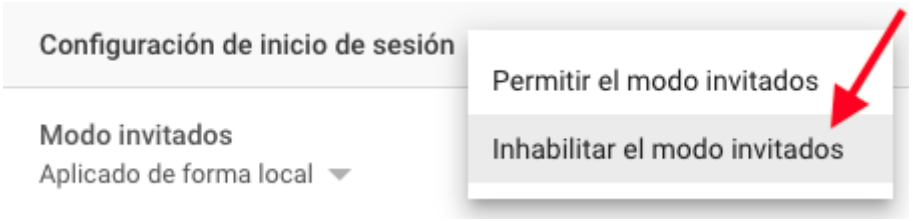
- **Obligation de réinscrire** l'enregistrement : forcer la relecture de l'enregistrement de l'appareil avec les identifiants de l'utilisateur lorsque ses données sont supprimées
- **Powerwash:** ne pas activer la fonction Powerwash

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.**

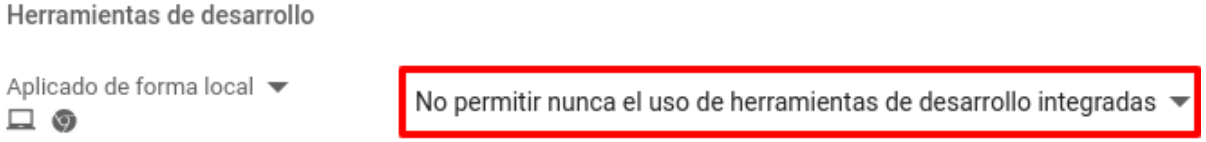
Nous sélectionnerons l'Unité Organisationnelle où nous voulons appliquer les changements. Nous cherchons la section appelée **Paramètres de connexion** et dans le paramètre **"Mode invité"** nous avons marqué **"Désactiver le mode invité"**. Pour enregistrer les modifications, nous cliquerons sur le 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:



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

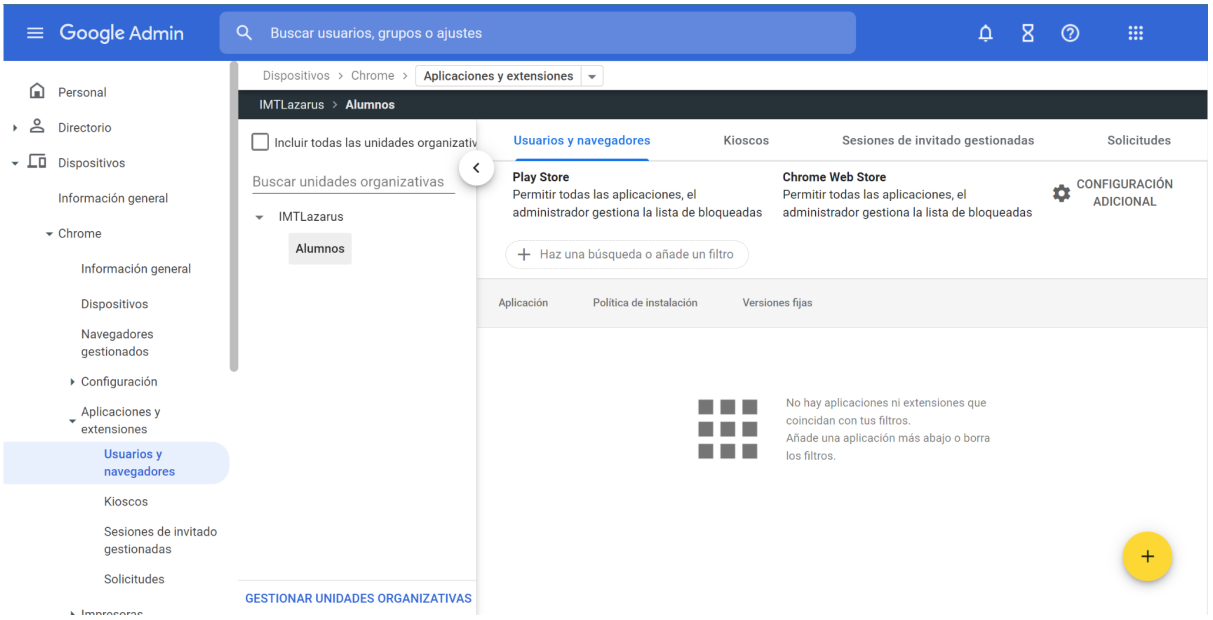
Depuis la console de gestion de Google Workspace, nous pouvons désactiver à la fois la ressource de l'appareil photo au niveau matériel (complètement désactivé) ou restreindre l'application native de l'appareil photo, mais à son tour permettre son utilisation dans les sessions de Google Meet et permettre 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**

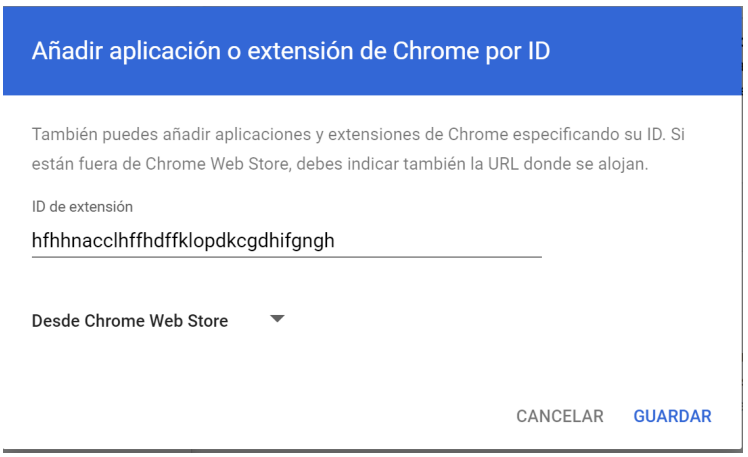
Nous gardons la dernière partie de l'ID: **hfhhnacclhffhdffklopdkcgdhifgngh**

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.

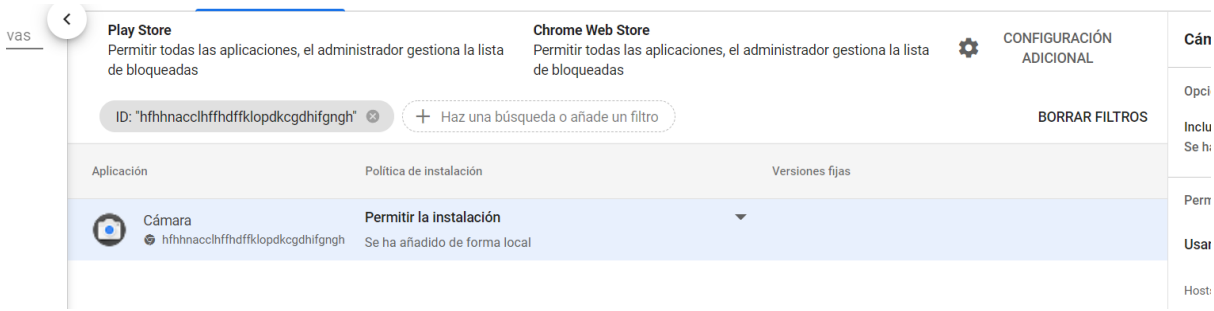


Cliquez sur le **Bouton + jaune > Ajouter l'application ou l'extension Chrome par ID**

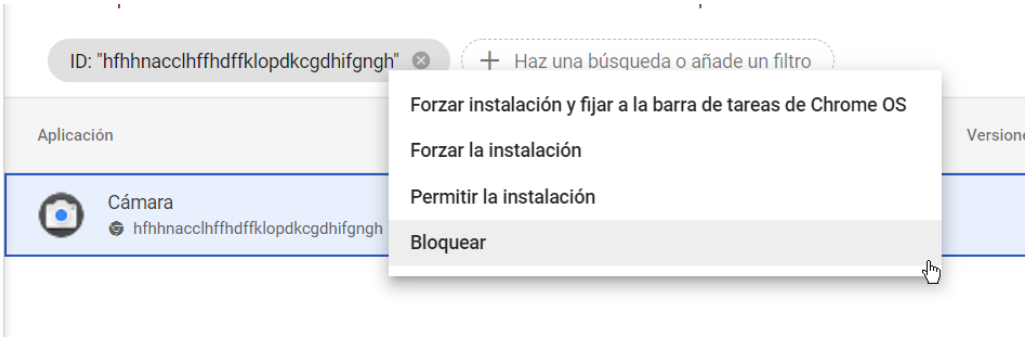
Dans la fenêtre qui s'ouvre, nous saisissons l'ID de l'application de la caméra que nous avons obtenue précédemment: **hfhhnacclhffhdffklopdkcgdhifgngh** et nous cliquons sur **ENREGISTRER**



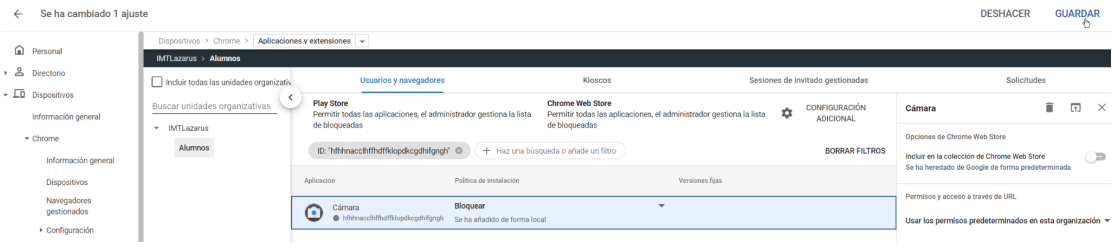
Après avoir ajouté:



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



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

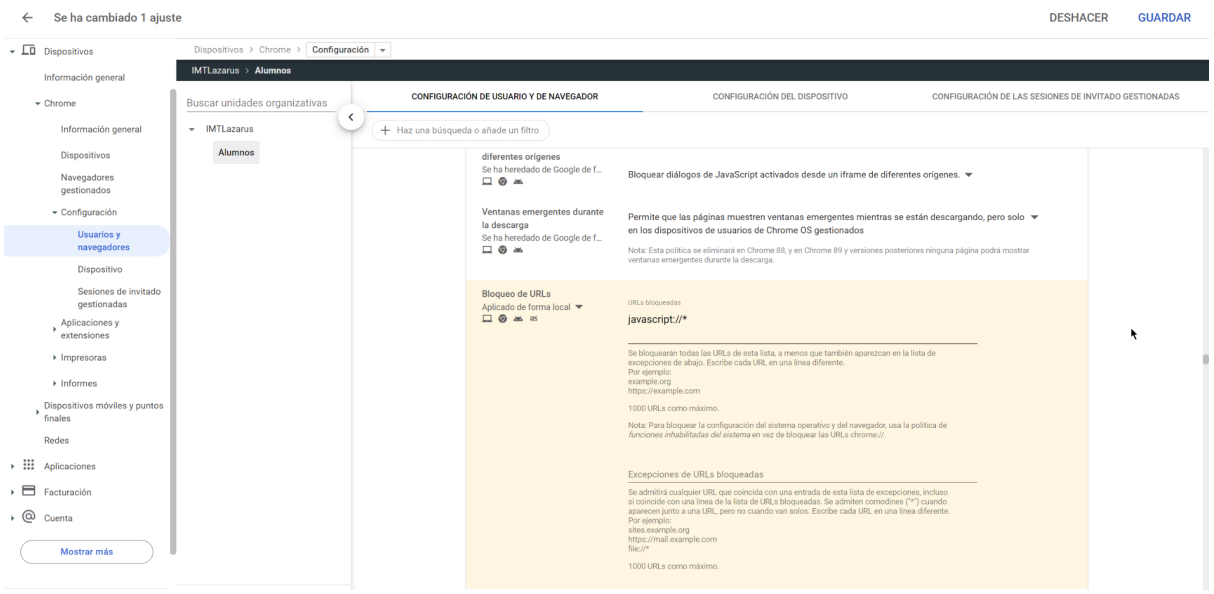


8. Désactiver l’exécution de javascript dans la barre du navigateur:

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.

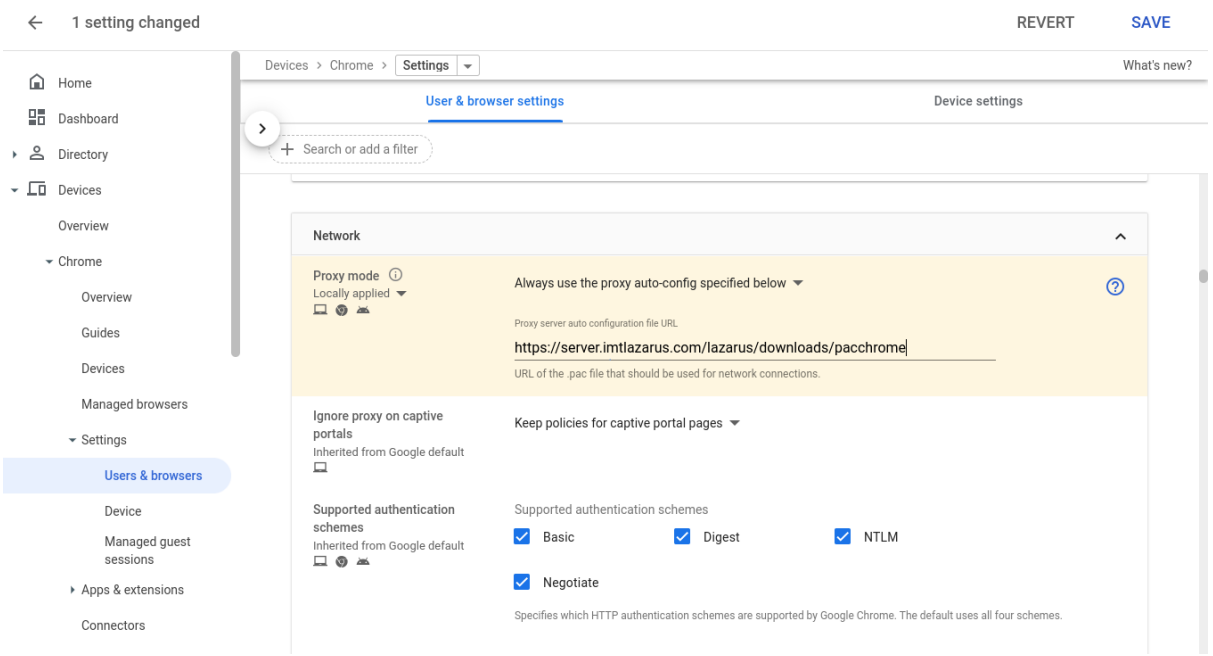
Dans **Verrouillage URLs**, nous ajoutons **javascript://*** et nous cliquons sur **ENREGISTRER** en haut.



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



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