



PC PUMA

PROGRAMA DE CONECTIVIDAD MÓVIL

INSTITUTO TECNOLÓGICO DE PUEBLA
INSTITUTO TECNOLÓGICO DE PUEBLA
INSTITUTO TECNOLÓGICO DE PUEBLA



**UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
SECRETARÍA DE DESARROLLO INSTITUCIONAL**



Proyecto PC Puma

Manual de enrolamiento MDM y puesta a punto de dispositivos v.1.4

Elaboró:
Amado Esparza Martín del Campo

Revisó:
Ing. Francisco Adolfo López Suárez

MARZO 2020



ÍNDICE

OBJETIVO	3
REQUERIMIENTOS	3
ENROLAMIENTO DE DISPOSITIVOS	4
Cuenta MDM administrativa	4
Creación de una red a administrar	4
DISPOSITIVOS IOS	6
Asignar configuración	7
Creación de Tag	10
Creación de Perfil	13
Wallpaper	16
Restricciones	17
Sección Apple restrictions	19
Sección iOS Supervised restrictions	22
Sección Windows 10 restrictions de iPad	25
Privacidad y Bloqueo	26
Aplicaciones	27
Asignación del Perfil de Administración a las iPads	30
Asignación de red al perfil de configuración	32
Encendido del iPad	35
DISPOSITIVOS WINDOWS 10	38
Creación de cuenta para préstamo	38
Enrolamiento	38
Instalación de Agente	42
Verificación de enrolamiento	43
DISPOSITIVOS CHROME OS	44
Enrolamiento de dispositivos	44
Puesta a punto de Chromebooks	44
Unidades organizativas	44
Creación de Usuario para administración	47
Configuración de usuario y navegador	49
Configuración de dispositivo	69
Gestión de aplicaciones a instalar	78
Asignación de Dispositivos a unidades organizativas	84
Powerwash	87



OBJETIVO

Indicar los pasos para realizar el enrolamiento de dispositivos para la administración remota y establecer los parámetros necesarios en la plataforma MDM para realizar el préstamo de dispositivos del proyecto PC PUMA.

REQUERIMIENTOS

Se deberá de contar con lo siguiente para el enrolamiento de dispositivos:

- Adquisición de las licencias de MDM de Cisco Meraki, contar los números de serie de licencias
- Cuenta de administración en el dashboard de Cisco Meraki *
- Dispositivos a enrolar **
- En el caso de los dispositivos iOS, haber realizado la adquisición de los mismos con el DEP de la UNAM (10268733). Adicionalmente, contar con acceso a la plataforma Apple School Manager. Para mayor información, consultar el **Manual de gestión de Apple School Manager v1** elaborado por la CPTI.
- Se deberá contar con la licencia para enrolar las chromebooks*

*Cuenta de administración del dashboard entregada por la CPTI

**los dispositivos Chrome OS se enrolan a la consola de Google



ENROLAMIENTO DE DISPOSITIVOS

1. Cuenta MDM administrativa

Se debe solicitar a la CPTI el acceso administrativo el cual será mandando por correo el cual se contempla para uso de administrador.

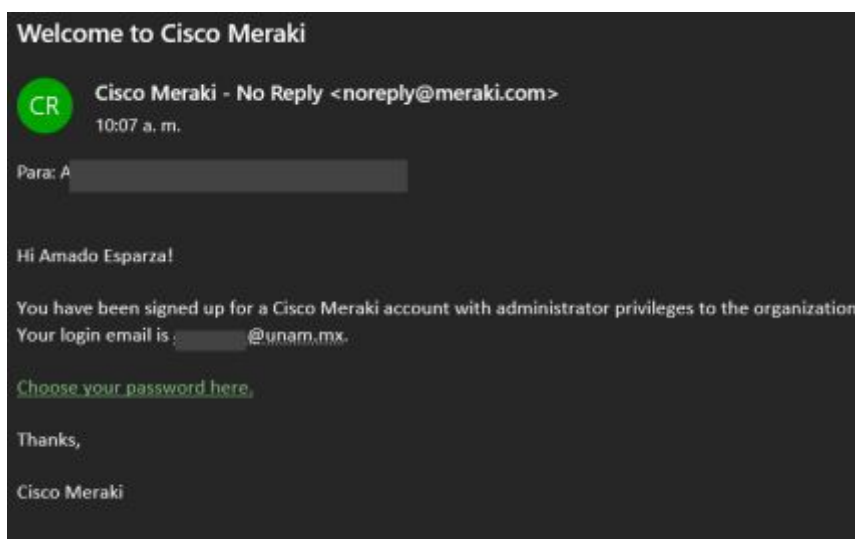


Imagen 1: Correo de invitación de privilegios de administrador MDM

2. Creación de una red a administrar

Una vez habiendo creado una cuenta y suministrando el password deseado para esta, el administrador deberá ingresar a un navegador (Chrome | Safari | Firefox) para realizar el enrolamiento de los dispositivos:

- <https://dashboard.meraki.com>

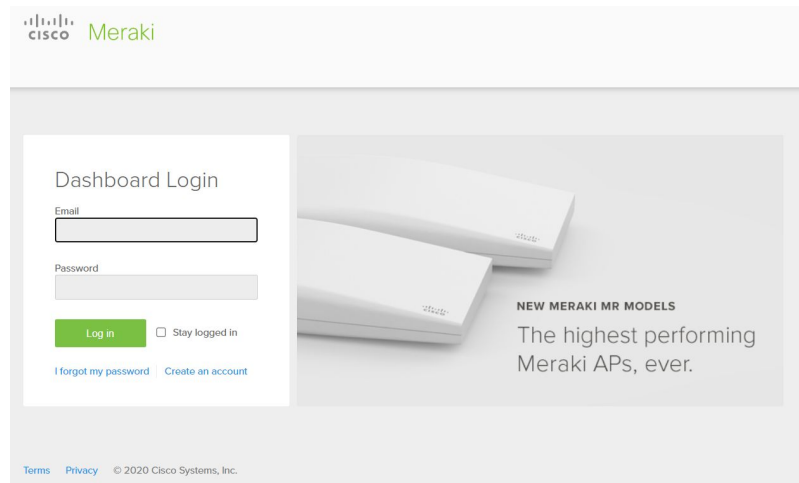


Imagen 2 : Dashboard Login Cisco Meraki

Dentro del dashboard de Cisco Meraki se creará una red para realizar la administración de los dispositivos, para ello ingresamos a NETWORK

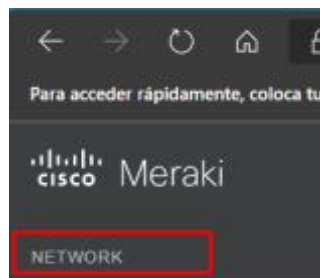


Imagen 3: extremos superior izquierdo del dashboard de Cisco Meraki

Enseguida vamos a CREATE NETWORK donde se añadirán las características básicas de la red.

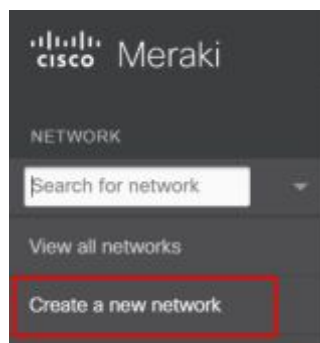


Imagen 4: Crear una nueva red

Se agrega el nombre “MDM -Fam” como ejemplo práctico en la casilla de **Network name**, el nombre de red en este apartado deberá ser el que la entidad considere necesario.



Q Search Dashboard

Create network

Setup network

Networks provide a way to logically group, configure, and monitor devices. This is a useful way to separate physically distinct sites within an Organization. ⓘ

Network name

Network type

Network configuration ☒ Default Meraki configuration

☐ Bind to template No templates to bind to ⓘ

☐ Clone from existing network

Imagen 5 : Setup Network

Seleccionamos **Create network** para crear la nueva red.

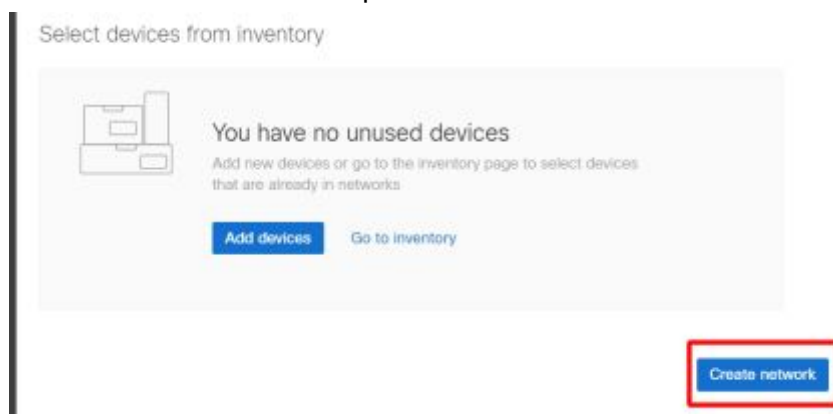


Imagen 6: Creación de Red

DISPOSITIVOS IOS

Para realizar el enrolamiento correcto de dispositivos iOS es importante no encender las ipads hasta que se haya terminado de configurar totalmente siguiendo este manual.

Para el enrolamiento correcto de los dispositivos IOS la entidad deberá de haber realizado los pasos necesarios del **Manual de Enrolamiento de ipads v.1** anteriormente a realizar los pasos de este manual pues menciona el procedimiento de agregar licencias Device Enrollment Program .



Los puntos 1 y 2 de **Enrolamiento de dispositivos** de este manual, se debe llevar a cabo el enrolamiento de IOS con los pasos que se describen a continuación en Asignar configuración , creación de tag, creación de Perfil .

Asignar configuración

Enseguida en la misma pestaña de la red creada “MDM -FAM” seleccionar **System Manager** y en el apartado **MANAGE** seleccionar **DEP**.

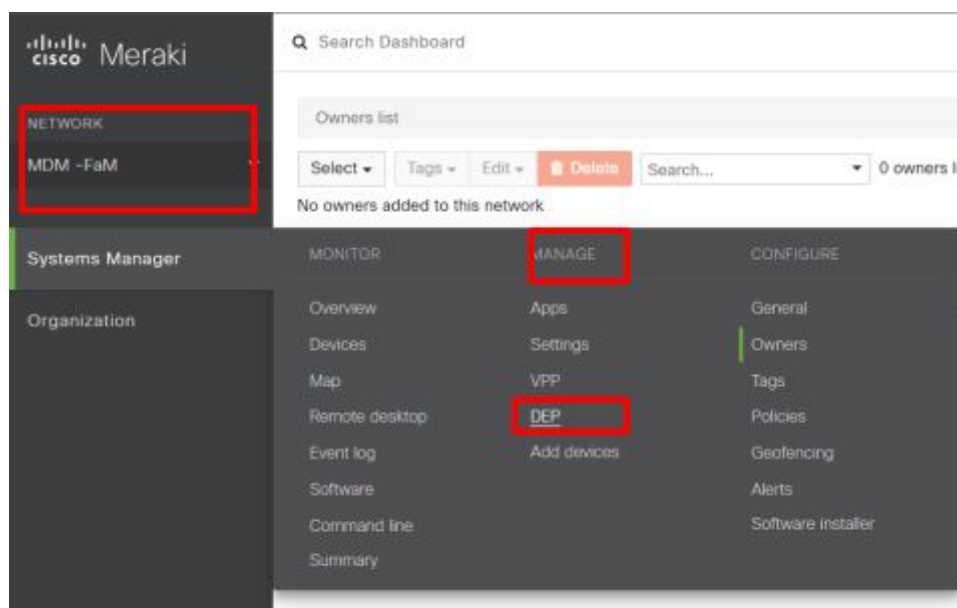


Imagen 7: Device Enrollment Program

Seleccionamos todas las ipads y en el apartado “**Assign settings**” seleccionamos **New**

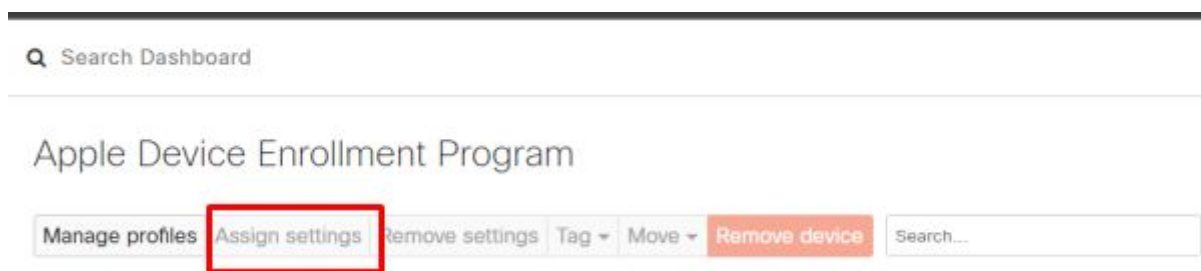


Imagen 8: Añadiendo configuración

Se le asigna FaM como ejemplo y se llenan los campos dependiendo de los datos de la entidad como se muestra en el siguiente ejemplo:



Profile details

Name	FaM
Support phone number ⓘ	5551913077
Support email address ⓘ	cvaldez@fam.unam.mx
Department ⓘ	Centro de Tecnologías de la Información

Options

Supervise ⓘ	Yes
Supervising host certificates ⓘ	<div>Choose File</div>
Allow Pairing ⓘ	Yes
Mandatory ⓘ	Yes
Removable ⓘ	<input type="checkbox"/>

Imagen 9: Llenado de datos para asignar configuración

Dentro del apartado **Skip** existen pasos que se pueden saltar al inicio del dispositivo

Allow Pairing ⓘ	Yes
Mandatory ⓘ	Yes
Removable ⓘ	<input type="checkbox"/>
Skip ⓘ	<div>Choose setup steps to skip</div>
Enrollment Redirect URL ⓘ	
Shared iPad	

Imagen 10: Apartado skip de exclusiones



Se deberán establecer en el apartado **Skip** se las siguientes exclusiones:

* Apple ID (iOS, macOS, tvOS)	* Apple Watch Migration (iOS)	
* Apple Pay (iOS, macOS)	* Cellular Plan (iOS)	
* Choose Your Look (iOS, macOS)	* Device to Device Migration (iOS)	
* Diagnostics (iOS, macOS, tvOS)	* FileVault (macOS)	
* Get Started (iOS)	* Home Button (iOS)	* iCloud Diagnostics (macOS)
* iCloud Documents and Desktop (macOS)	* iMessage and Facetime (iOS)	
* Keyboard Selection (iOS)	* Move from Android (iOS)	
* On-boarding screens (iOS)	* Passcode (iOS)	
* Privacy (iOS, macOS, tvOS)	* Registration (macOS)	
* Restore from Backup (iOS, macOS)	* Screensaver (tvOS)	
* Screen Time (iOS, macOS)	* Zoom Setup (iOS)	
* Where is this Apple TV? (tvOS)	* TV provider sign in screen (tvOS)	
* Siri (iOS, macOS, tvOS)	* TV home screen layout (tvOS)	
* Software Update (iOS)	* Tap To Setup Up (tvOS)	
* Terms and Conditions (iOS, macOS, tvOS)	* Touch ID (iOS, macOS)	
* True Tone (iOS, macOS)		

Imagen 11: Pasos a saltar al inicio del dispositivo

Location Services (iOS, macOS) es una opción la cual no queremos que salte este paso para poder contar con el servicio de ubicación,, así que no debe quedar dentro de la lista de pasos a saltar al inicio del iPad, del mismo modo quedan sin marcar:

- **Device to device migration (iOS)**
- **Get started (iOS)**
- **iCloud Diagnostics (macOS)**
- **Where is the apple TV? (tvOS)**
- **True Tone (iOS, macOS)**



Los cuales son opciones necesarias para poder enrolar de forma correcta las iPad al MDM de Meraki.

Terminando de escoger las opciones necesarias damos click en **Assign**

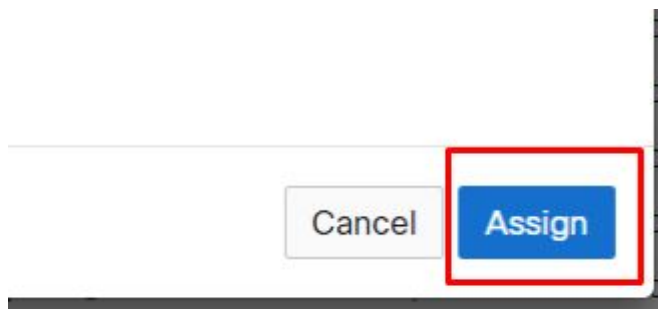


Imagen 12: Paso final para asignación de configuración

Creación de Tag

En el dashboard de Cisco Meraki, seleccionamos **NETWORK** y seleccionamos la red previamente creada "MDM -FaM" y vamos a la pestaña System Manager

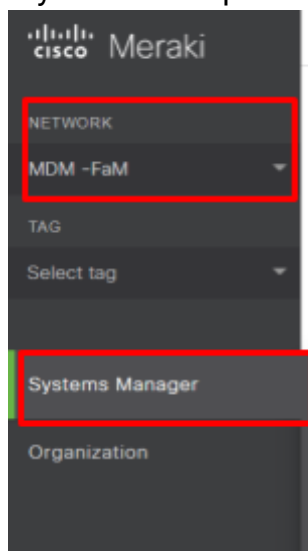


Imagen 13: Network -> System Manager

En la sección **CONFIGURE** seleccionar **Tags**

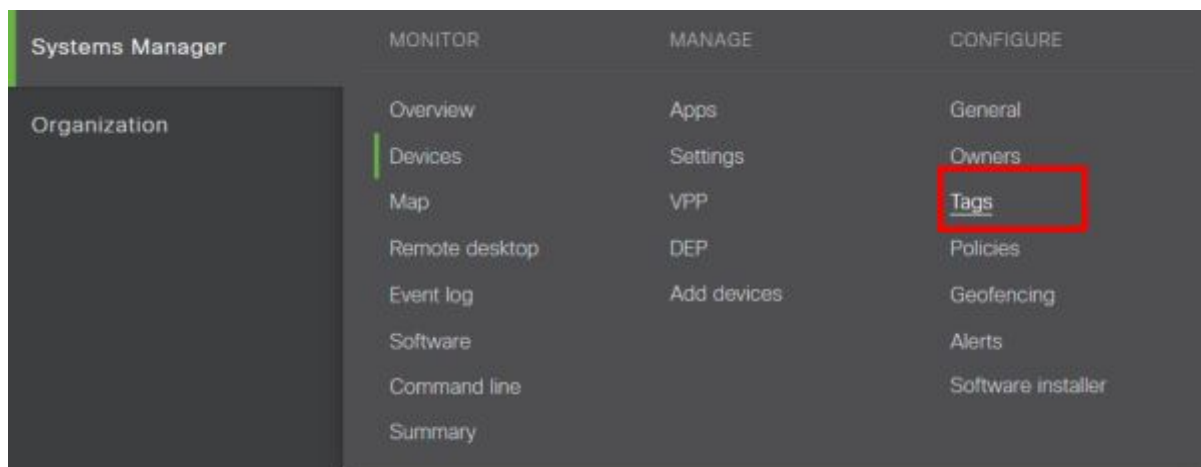


Imagen 14: Configuración de Tags

En la interfaz de Tags dar click en el botón de **+Add tag** para añadir el tag

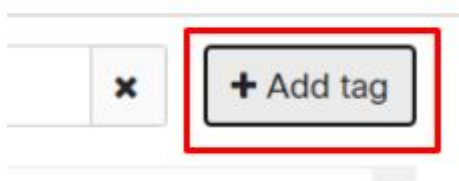


Imagen 15: Añadir tag

Seleccionar **Manual Tag** para aplicar a los dispositivos y dar click en Next

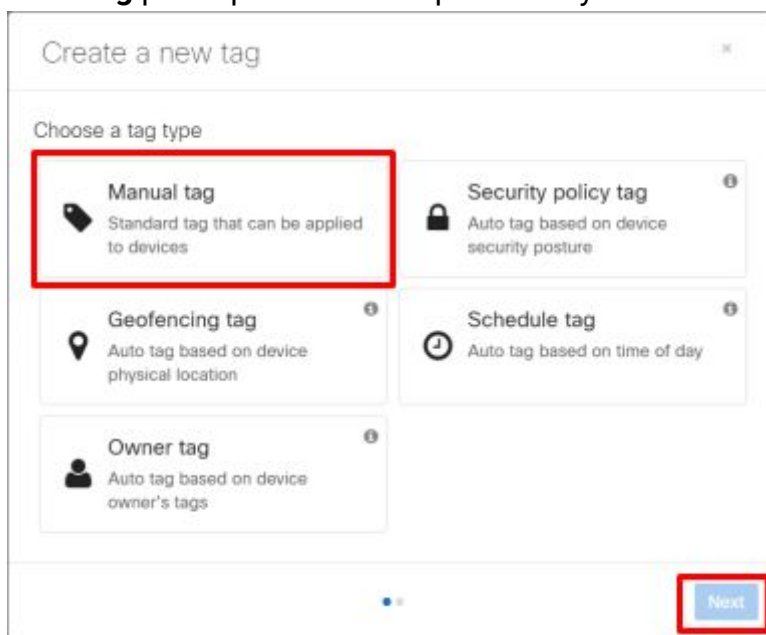


Imagen 16: Añadir Manual Tag



Se añade un nombre de tag, de manera de ejemplo se añade el nombre del Tag como "BASE", la entidad podrá elegir el nombre de tag que requiera.

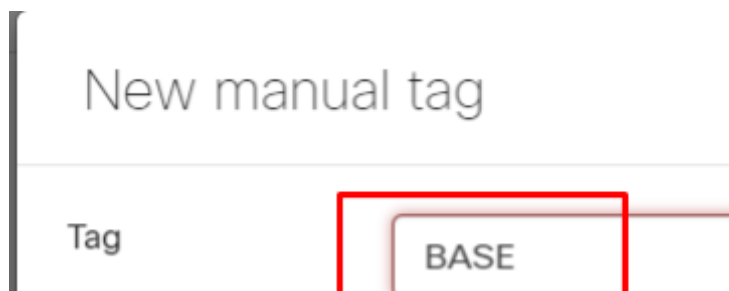


Imagen 17: Añadir nombre del Tag

Aquí deberá añadirse el ipad o ipads que se requieran añadir a este tag añadidas anteriormente mediante el **Manual de Enrolamiento de ipads v1**

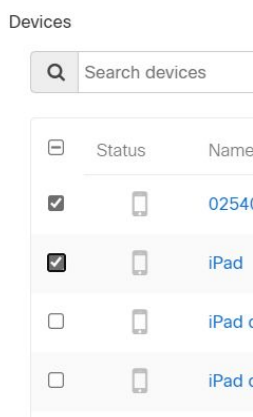


Imagen 18: ipads a agregar a tag

Una vez habiendo elegido las ipads a agregar al tag damos click en **Continue**

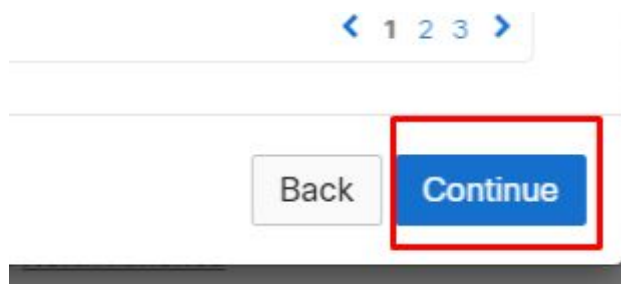


Imagen 19: Finalizar de añadir ipad a tag



Se deben guardar los cambios para terminar de añadir el Tag que se ha creado



Imagen 20: Guardar cambios

Creación de Perfil

El perfil se crea para implementar reglas que deberán

En el dashboard de cisco meraki ingresamos a **NETWORK** y seleccionamos la red previamente creada "MDM -FaM"

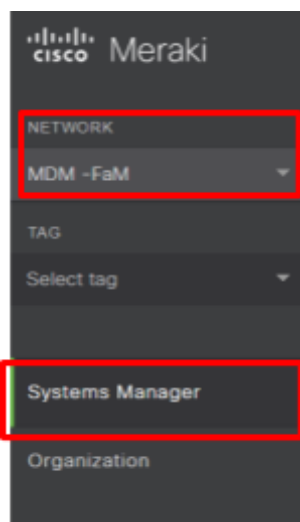


Imagen 21: Network -> "MDM-FaM" -> System Manager

Seleccionamos en la sección de **MANAGE** la opción **Settings** para comenzar a añadir un perfil

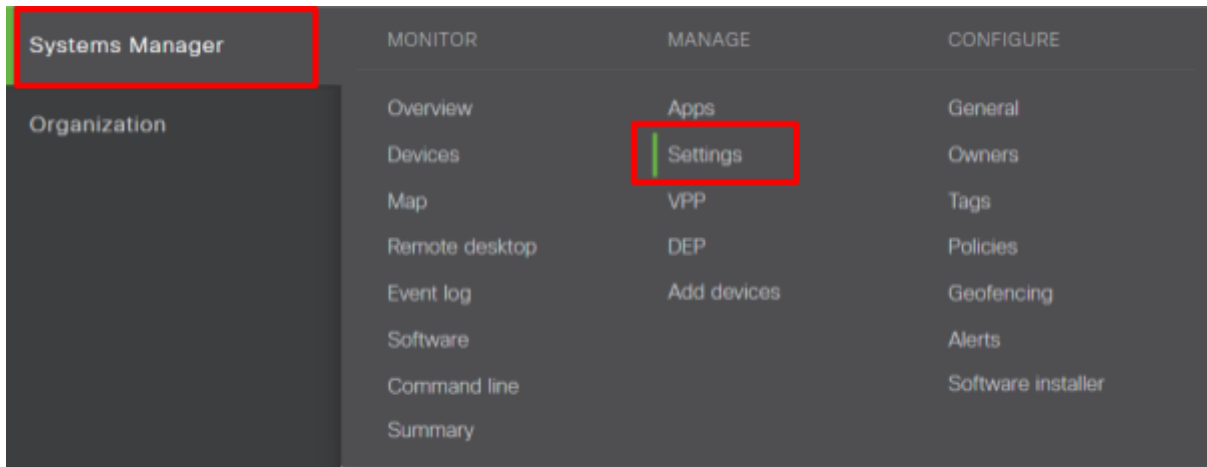


Imagen 22: Ingresar en Settings de Systems Manager para añadir perfil

y damos click en **+ Add Profile**

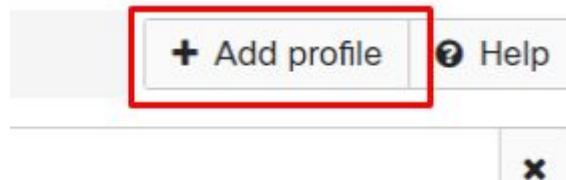


Imagen 23: Añadir perfil

En la ventana de **Add Profile** seleccionar **Standard Device profile (default)** y dar click en **Continue**

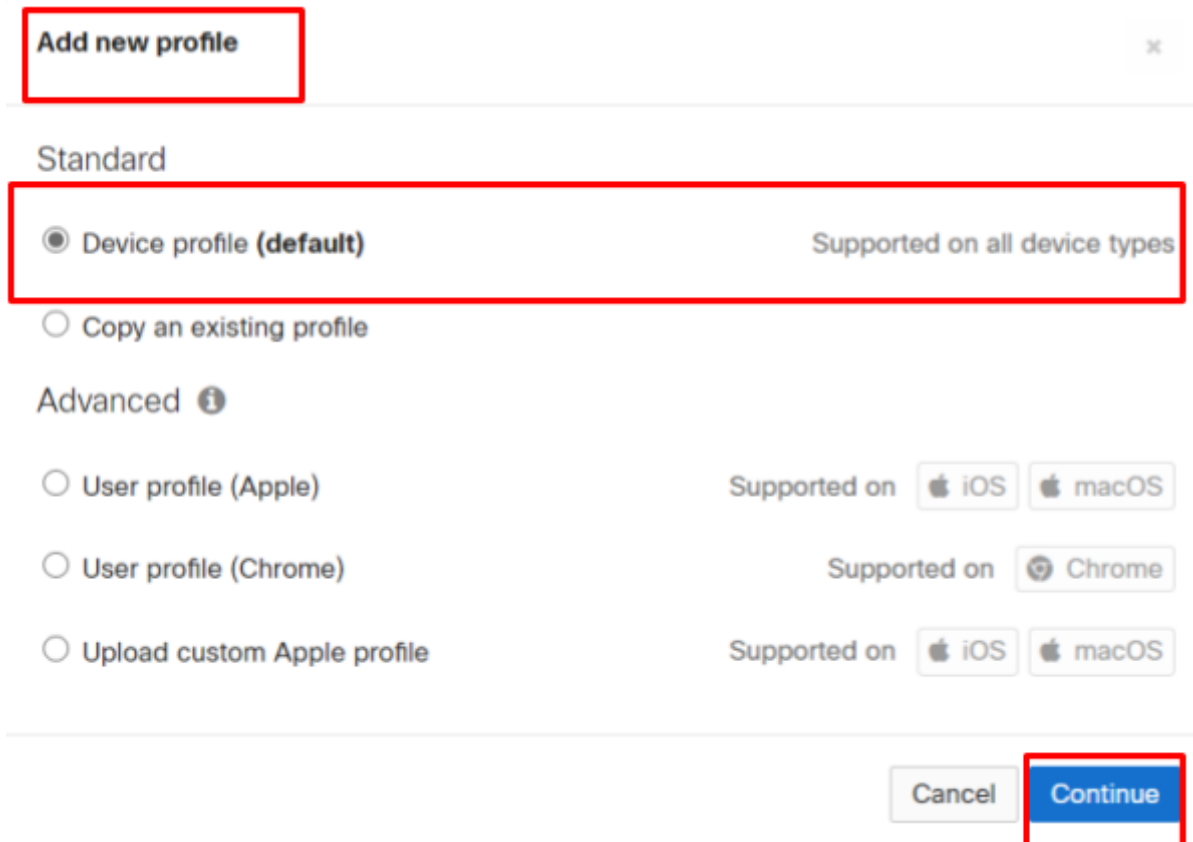


Imagen 24: Seleccionar Device profile



Se utiliza en forma de ejemplo “PERFIL-PRESTAMO” en el campo Name, la entidad podrá elegir el nombre de perfil de préstamo que requiera.

Imagen 25: Agregar nombre de perfil en el campo Name

En el apartado **Targets** seleccionar el campo **with ANY of the following tags**

Imagen 26: El alcance serán los siguientes tags

En la opción **Device tags** escoger el tag previamente creado “BASE” , aquí debería seleccionarse el nombre del tag creado por la entidad.

Imagen 27: Device tags

La configuración debería quedar de la siguiente forma:



Type

Device profile

Name

PERFIL-PRESTAMO

The name that will be shown to users

Description

Optional

Profile Removal Policy

Removal Policy ⓘ

Allow users to remove this profile

Targets

Group type

Manual Named Configure tags

Scope

with ANY of the following tags

Device tags

BASE

Device type, manual tags

Policy tags

Select policy tags

Imagen 28: Configuración completa del perfil

Guardar los cambios para salvar el perfil que se ha creado.

Remove

Delete this profile

Cancel Save

(Please allow 1-2 minutes for changes to take effect.)

Imagen 29: Guardar cambios del perfil

Wallpaper

En esta sección se añadirá la opción de incluir un wallpaper predeterminado para los dispositivos iOS en préstamo.

Dentro del misma interfaz de perfil dar click en **+Add settings** buscar **iOS Wallpaper** en el apartado IOS de **Add new settings payload** y seleccionar la opción para configurar:

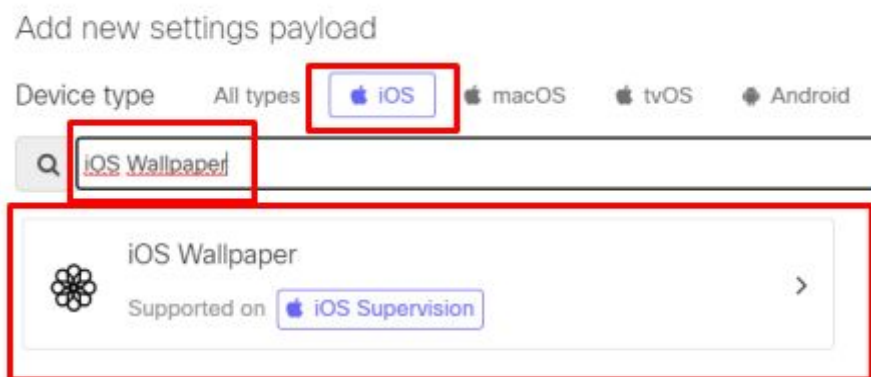


Imagen 30: opción iOS Wallpaper

Seleccionar la imagen de fondo provista para PC PUMA para la entidad y guardar dando clic en **Save**

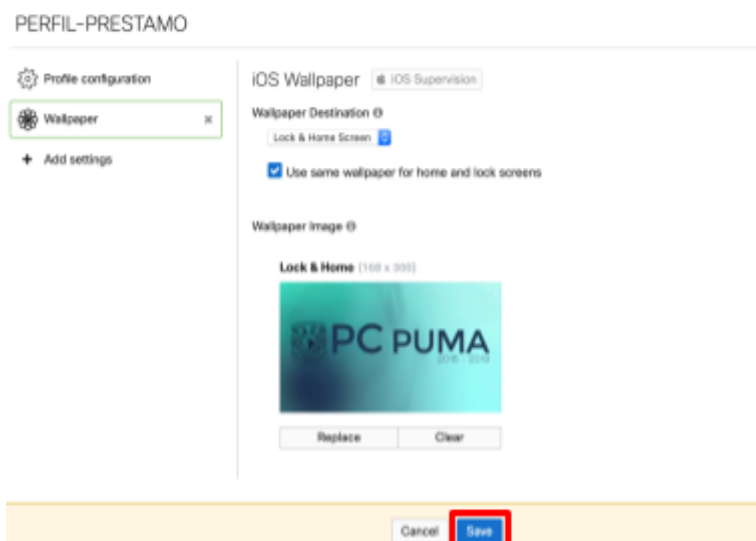


Imagen 31: salvar configuración iOS Wallpaper


Restricciones

En esta sección se añadirán reglas que servirán para la administración de dispositivos IOS tales como:

- Sincronización
- Aspectos de interfaz gráfica
- Certificados de seguridad
- Aplicaciones
- Acceso de usuario

Se añade una nueva configuración en la interfaz de "PERFIL- PRESTAMO" para lo que se seleccionar nuevamente **+Add settings**

PERFIL-PRESTAMO

 Profile configuration


 Add settings

Imagen 32: Añadir nueva configuración

Se busca en el apartado que contiene la lupa la opción de Restrictions que aparecerá enseguida y se selecciona

Add new settings payload

Device type  iOS  macOS  tvOS  Androic



Restrictions



Supported on

 iOS

 macOS

 tvOS

 Android



 Windows

Imagen 33: Seleccionar opción Restrictions para añadir configuración

Una vez dentro de la opción a configurar **Restrictions** las opciones a marcar deberán quedar de esta forma en las diferentes secciones :

- Sección **Cross-platform restrictions**



Restrictions Help

Device type All types iOS macOS tvOS Android Windows

Cross-platform restrictions

Camera

☒ Allow use of camera ⓘ iOS macOS Android Windows

Device functionality

☐ Allow installing apps ⓘ iOS Supervised Android

☒ Allow screen capture iOS Windows macOS 10.14.4+

☐ Allow device assistant (Siri/Cortana) iOS Windows

Imagen 34: Opciones a marcar en sección Cross-platform restrictions

- Sección **Apple restrictions**



Apple restrictions

Device functionality

- ☐ Allow voice dialing 
- ☒ Allow automatic sync when roaming 
- ☒ Allow Passbook notifications while locked 
- ☐ Allow in-app purchases 
- ☒ Allow iTunes file sharing services 
- ☐ Force user to enter iTunes Store password for all purchases 
- ☒ Show Control Center in lock screen 
- ☒ Show Notification Center in lock screen 
- ☒ Show Today view in lock screen 
- ☒ Allow remote screen observation by the Classroom app  
- ☒ Do not containerize work data and contacts from unmanaged apps 
- ☒ Do not containerize personal data and contacts from managed apps 
- ☒ Allow Handoff  
- ☒ Require passcode on outgoing AirPlay pairing requests 
- ☒ Require passcode on incoming AirPlay pairing requests 
- ☐ Force paired Apple Watch to use Wrist Detection 
- ☐ Disallow sharing of managed documents with AirDrop 
- ☒ Allow pairing with Remote app or Control Center widget 
- ☐ Allow managed apps to write contacts to unmanaged contacts accounts 
- ☐ Allow unmanaged apps to read from managed contacts accounts 
- ☒ Allow server-side Siri logging 



iCloud

iOS & macOS

- ☒ Allow iCloud Photo Library  

iCloud

iOS

- ☐ Allow backup of enterprise books 
- ☐ Allow notes and highlights sync for enterprise books 



☐ Allow photo stream

☐ Allow managed app to store data in iCloud

iCloud

macOS

☒ Allow Back to My Mac

☒ Allow Find My Mac

☒ Allow Bookmark sync

☒ Allow Mail sync

☒ Allow Calendar sync

☒ Allow Reminder sync

☒ Allow Address Book sync

☒ Allow Notes sync

☒ Allow desktop and document sync

Security and privacy

☒ Allow diagnostic data to be sent to Apple

☒ Allow user to accept untrusted TLS certificates

☐ Force encrypted backup

☒ Allow automatic updates to certificate trust settings

☐ Force limited ad tracking

☒ Allow Touch ID to unlock device

Ratings region

United States

Allowed content ratings

Specify allowed ratings for the following content

Movies: Allow All Movies

TV Shows: Allow All TV Shows

Apps: Allow All Apps

Software updates

☐ Delay OS software updates

Imagen 35: Opciones a marcar en sección Apple restrictions



- Sección iOS Supervised restrictions

iOS Supervised restrictions

About Supervision

These restrictions only have an effect when a device is in 'supervised' mode. This mode can only be enabled with DEP or Apple Configurator. [Read more](#)

Applications

- ☒ Allow app removal 🍏 iOS
- ☐ Allow use of iTunes Store 🍏 iOS
- ☒ Allow use of Safari 🍏 iOS
- ☐ Enable autofill 🍏 iOS 🍏 macOS 10.13+
- ☐ Force fraud warning
- ☒ Enable javascript
- ☒ Allow popups
- ☐ Allow FaceTime 🍏 iOS
- ☐ Allow iMessage 🍏 iOS 6+
- ☐ Allow Game Center 🍏 iOS 6+ 🍏 macOS 10.13+
- ☐ Allow Bookstore 🍏 iOS 6+
- ☐ Allow Bookstore erotica 🍏 iOS 🍏 tvOS 11.3+
- ☐ Allow Podcasts 🍏 iOS 8+
- ☐ Allow App Store 🍏 iOS 9+
- ☐ Allow News app 🍏 iOS 9+
- ☒ Allow Apple Music 🍏 iOS 9.3+
- ☐ Allow Apple Music Radio 🍏 iOS 9.3+

Allowed Single App Mode ⓘ

Choose an app ▼

Show or hide apps

Allow all apps ⬇

Device functionality



☒ Allow UI configuration profile installation ⓘ iOS 6+

☐ Allow adding Game Center friends iOS macOS 10.13+

☐ Allow modifying account settings iOS 7+

☒ Allow AirDrop iOS 7+ macOS 10.13+

☐ Allow changes to cellular data usage for apps iOS 7+

☐ Allow user-generated content in Siri iOS 7+

☒ Allow Find My Device in the Find My app. iOS 13+ Supervised

☒ Allow Find My Friends in the Find My app. iOS 13+ Supervised

☒ Allow modifying Find My Friends settings iOS 7+

☒ Allow host pairing iOS 7+

☐ Allow multiplayer gaming ⓘ iOS macOS 10.13+

☒ Force Wi-Fi power on iOS 13+ Supervised

☐ Enable Siri profanity filter iOS

☒ Allow Files Network Drive Access iOS 13+ Supervised

☒ Allow Files USB Drive Access iOS 13+ Supervised

☐ Allow configuring restrictions iOS 8+

☐ Allow Erase All Content and Settings iOS 8+

☐ Allow Internet results in Spotlight iOS 8+ macOS 10.11+

☐ Allow keyboard auto-correction iOS 8.1.3+

☐ Allow keyboard spell-check iOS 8.1.3+

☒ Allow definition lookup iOS 8.1.3+ macOS 10.11.2+

☒ Allow predictive keyboard iOS 8.1.3+

☒ Allow continuous path keyboard iOS 13+ Supervised

☒ Allow keyboard shortcuts iOS 9+

☐ Allow pairing with Apple Watch iOS 9+

☐ Allow modification of passcode settings ⓘ iOS 9+ macOS 10.13+

☐ Allow modification of device name iOS 9+ tvOS 11+

☒ Keep device name up-to-date with Dashboard ⓘ iOS 9+

☐ Allow modification of wallpaper iOS 9+ macOS 10.13+

☐ Allow automatic downloading of apps purchased on other devices iOS 9+



UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
SECRETARÍA DE DESARROLLO INSTITUCIONAL
Manual de enrolamiento MDM y puesta a punto de dispositivos v.1.4

☒ Automatically trust enterprise apps 🍏 iOS 9+

☒ Allow changes to Notifications settings 🍏 iOS 9.3+

☒ Allow modification of diagnostic submission and app analytics settings 🍏 iOS 9.3.2+

☐ Allow modification of Bluetooth settings 🍏 iOS 10+

☒ Allow dictation input 🍏 iOS 10.3+ 🍏 macOS 10.13+

☒ Enforce SSID whitelisting ⓘ 🍏 iOS 10.3+

☐ Automatically grant observation permission to teachers using Classroom app ⓘ 🍏 iOS 10.3+ 🍏 macOS 10.14.4+

☒ Allow AirPrint 🍏 iOS 11+

☒ Allow credential storage for AirPrint 🍏 iOS 11+

☐ Require trusted certificates for TLS printing communication 🍏 iOS 11+

☒ Allow iBeacon discovery of AirPrint printers 🍏 iOS 11+

☐ Allow removal of system apps 🍏 iOS 11+

☐ Allow creation of VPN configurations 🍏 iOS 11+

☐ Enable USB Restricted Mode ⓘ 🍏 iOS 11.3+

☐ Turn the Date & Time 'Set Automatically' feature to ON and disallow user disabling 🍏 iOS 12+ Supervised 🍏 tvOS 12.2+

☒ Allow users to use saved passwords in Safari and AutoFill Passwords feature ⓘ 🍏 iOS 12+ Supervised 🍏 macOS 10.14+

☒ Allow users device to request passwords from nearby devices 🍏 iOS 12+ Supervised 🍏 macOS 10.14+ 🍏 tvOS 12+

☒ Allow users to share their passwords with the Airdrop Passwords feature 🍏 iOS 12+ Supervised 🍏 macOS 10.14+ 🍏 tvOS 12+

☒ Allow users to add or remove a cellular plan to the eSIM on the device 🍏 iOS 12.1+ Supervised

☒ Allow users to modify the personal hotspot setting 🍏 iOS 12.2+ Supervised

iCloud
iOS

☐ Allow document sync ⓘ 🍏 iOS 🍏 macOS 10.11+

☐ Allow cloud Keychain sync ⓘ 🍏 iOS 7+ 🍏 macOS 10.12+

iCloud
iOS & macOS

☐ Allow backup ⓘ 🍏 iOS 5+



Content ratings



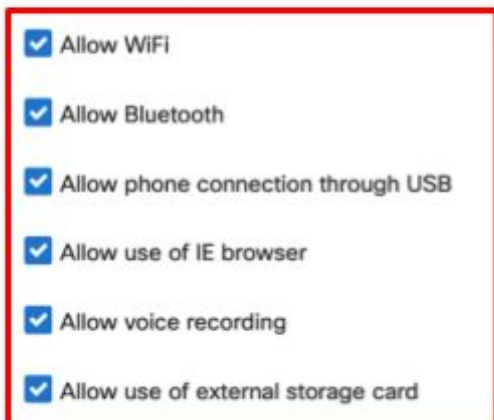
Imagen 36: Opciones a marcar en sección iOS Supervised restrictions

- Sección **Windows 10 restrictions** de iPad

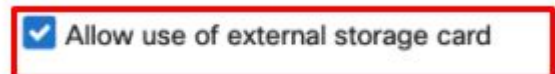
Elegir las siguientes opciones en esta sección y enseguida dar clic en **Save**

Windows 10 restrictions

Device functionality



☐ Encrypt device internal storage



☐ Encrypt device internal storage



Imagen 37: Opciones a marcar en sección Windows 10 restrictions y guardar



Privacidad y Bloqueo

En esta sección se configuran opciones como de rastreo del dispositivo en préstamo y bloqueo.

Se añade una nueva configuración en la interfaz de “PERFIL- PRESTAMO” para lo que se seleccionar nuevamente **+Add settings**

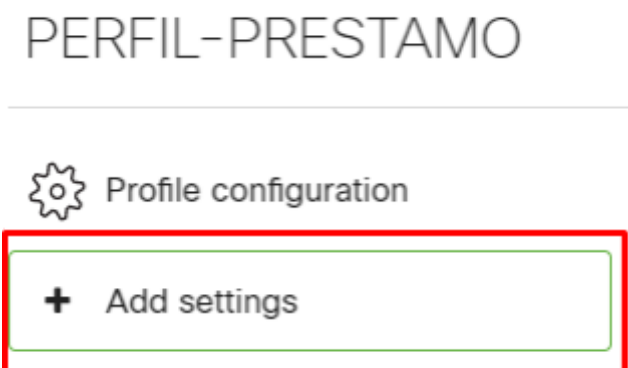


Imagen 38: Añadir nueva configuración

Se busca en el apartado que contiene la lupa la opción de **Privacy and Lock** que aparecerá enseguida y se selecciona:

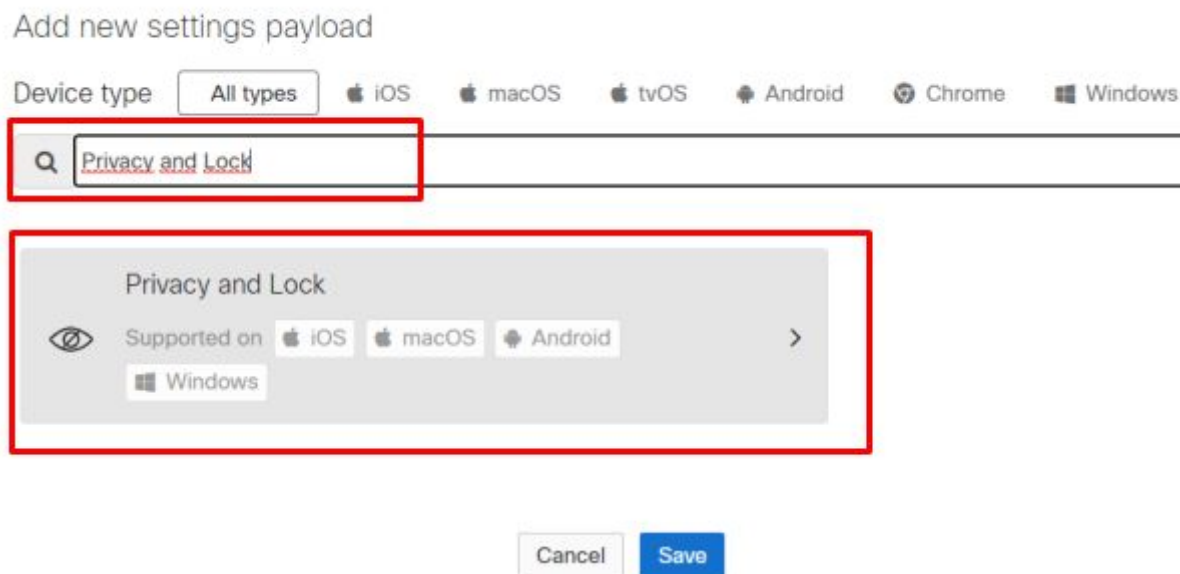


Imagen 39: Búsqueda de opción Privacy and Lock a configurar



Marcar las casillas de las siguientes opciones dentro de la sección Privacy and Lock

PERFIL-PRESTAMO

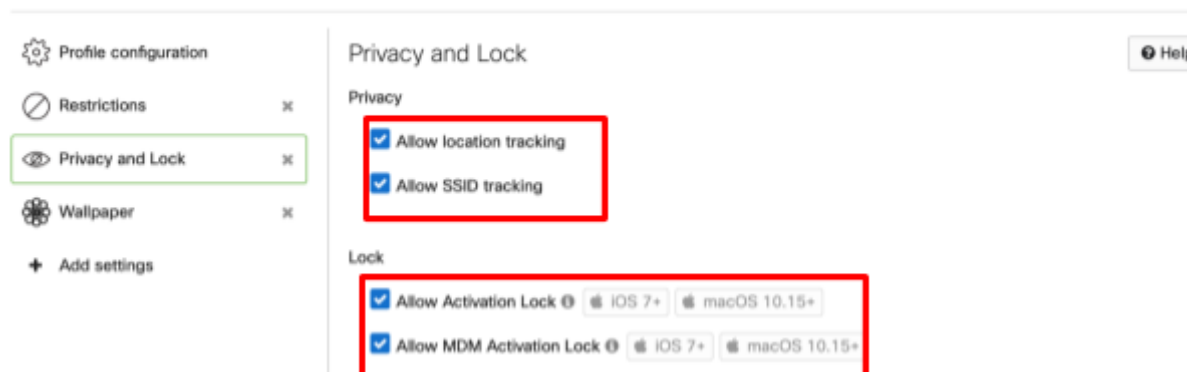


Imagen 40: Marcar casillas en sección Privacy and Lock

No olvidar guardar los cambios en la sección **Privacy and Lock** al terminar de marcar las casillas de verificación.



Imagen 41: Guardar cambios de Sección Privacy and Lock

Aplicaciones

En este apartado la entidad selecciona las aplicaciones que considere adecuadas para sus necesidades académicas para ello acudimos al dashboard de cisco meraki e ingresamos a **NETWORK** y seleccionamos la red previamente creada de ejemplo "MDM -FaM" y seleccionamos **System Manager**

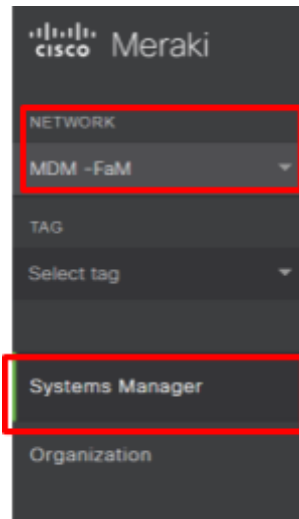


Imagen 42: Network -> "MDM-FaM" -> System Manager

En el apartado **Manage** seleccionamos la opción **Apps**

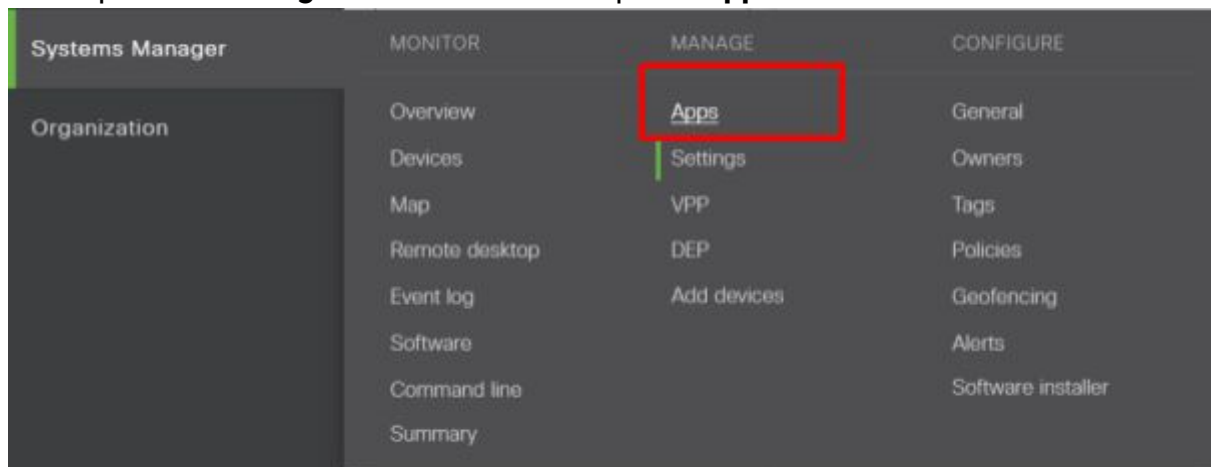


Imagen 43: Seleccionar Apps para añadir aplicaciones a instalar

Seleccionar **+Add an app**.

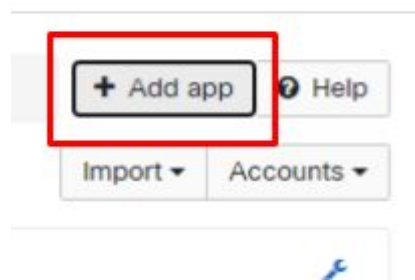


Imagen 44: Añadir aplicación



En la pantalla que se despliega para añadir la aplicación seleccionar **iOS** y el tipo de App **App Store App**

Add an app

App platform



App type

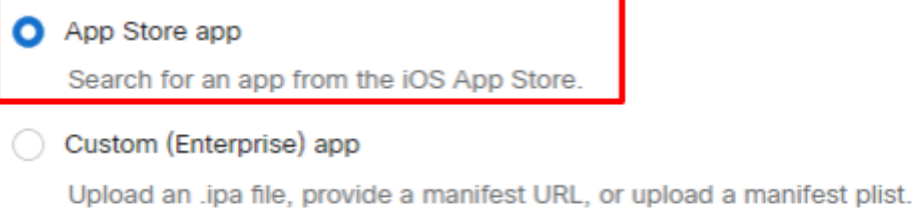


Imagen 45: Selección de plataforma de la app a instalar

Buscar la aplicación en el cuadro de búsqueda y elegir el país de la tienda: México y finalmente guardar dando clic al botón **Save**

Add new iOS app

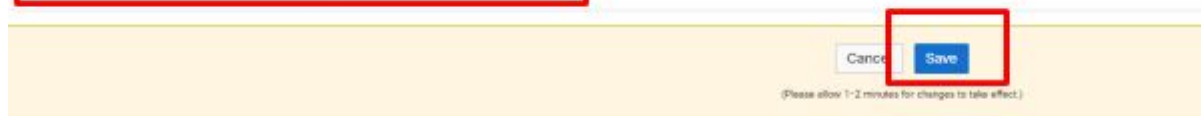


Imagen 46: Búsqueda de aplicaciones a instalar



Nota: Al seleccionar cada aplicación es necesario ir guardando los cambios para que se vayan añadiendo a la lista de aplicaciones a propagar en los dispositivos de la entidad.

Se establece la siguiente lista de aplicaciones base:

<input checked="" type="checkbox"/>	#	Icon	Name ▲	Platform	Type	Scope	Tags
<input checked="" type="checkbox"/>	1		Adobe Acrobat Reader for Docs	iOS	Store	with ANY of the following tags	BASE
<input checked="" type="checkbox"/>	2		Aula	iOS	Store	with ANY of the following tags	BASE
<input checked="" type="checkbox"/>	3		CalConvert: Calculadora CE	iOS	Store	with ANY of the following tags	BASE
<input checked="" type="checkbox"/>	4		Documentos de Google	iOS	Store	with ANY of the following tags	BASE
<input checked="" type="checkbox"/>	5		Dropbox	iOS	Store	with ANY of the following tags	BASE
<input checked="" type="checkbox"/>	6		Evernote	iOS	Store	with ANY of the following tags	BASE
<input checked="" type="checkbox"/>	7		Facebook	iOS	Store	with ANY of the following tags	BASE
<input checked="" type="checkbox"/>	8		Google Chrome	iOS	Store	with ANY of the following tags	BASE
<input checked="" type="checkbox"/>	9		Google Classroom	iOS	Store	with ANY of the following tags	BASE
<input checked="" type="checkbox"/>	10		Google Drive – almacenamiento	iOS	Store	with ANY of the following tags	BASE
<input checked="" type="checkbox"/>	11		Kahoot! Play & Create Quizzes	iOS	Store	with ANY of the following tags	BASE
<input checked="" type="checkbox"/>	12		Meraki Systems Manager	iOS	Store	All devices	
<input checked="" type="checkbox"/>	13		Messenger	iOS	Store	with ANY of the following tags	BASE
<input checked="" type="checkbox"/>	14		Microsoft Excel	iOS	Store	with ANY of the following tags	BASE
<input checked="" type="checkbox"/>	15		Microsoft PowerPoint	iOS	Store	with ANY of the following tags	BASE

Imagen 47: Aplicaciones base

Asignación del Perfil de Administración a las iPads

El perfil de DEP nos ayudará a asignar las iPads a administrar, para ello se selecciona **NETWORK** y enseguida la red que hemos creado para el ejemplo “MDM -FaM”

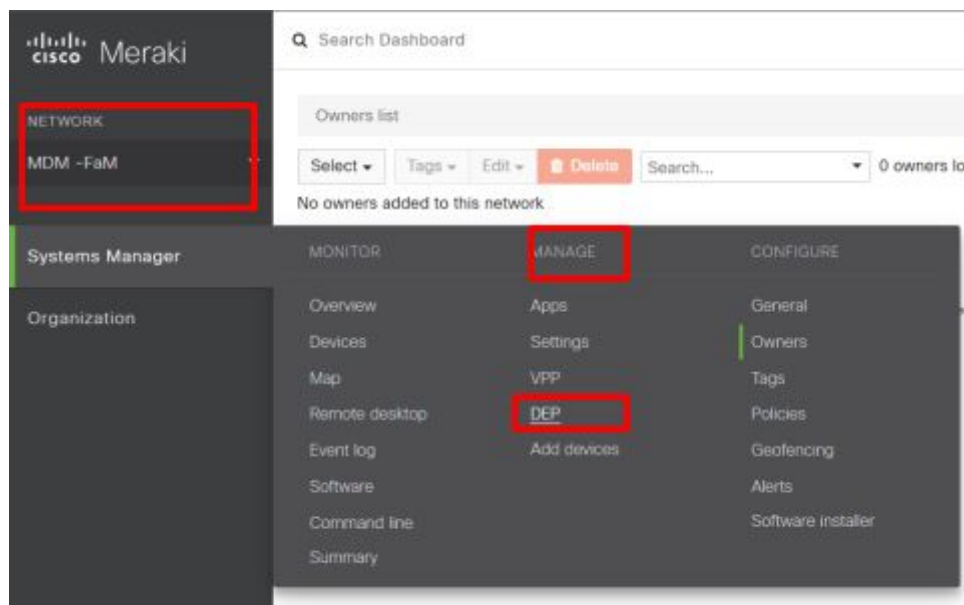


Imagen 48: Ruta para asignación de perfil de administración de iPad

En la interfaz de **Apple Device Enrollment Program** se marcan las casillas que la entidad requiera asignar al perfil de administración "FaM" que se ha creado anteriormente como ejemplo y damos clic en **Manage profiles**

Apple Device Enrollment Program

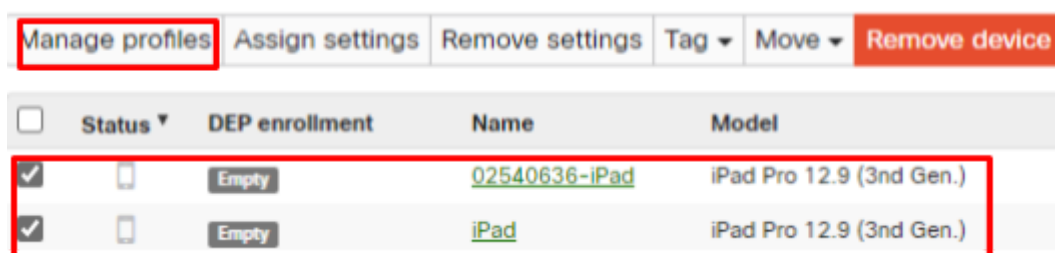


Imagen 49: Selección de dispositivos para asignar perfil de administración

Por último se selecciona la casilla del perfil de administración al cual se quieren asignar las iPads previamente seleccionadas y se da clic en **Update** quedando de esta forma enroladas a un perfil de administración



Manage Enrollment Profiles

Apple does not permit the deletion of DEP enrollment profiles once they have been created. Unchecking settings here will hide them from the assignment menu.

Show **Visible** All

<input checked="" type="checkbox"/>	Name	Visible ⓘ	Mandatory	Devices Assigned	Default ⓘ
<input checked="" type="checkbox"/>	FaM	Yes	Yes	0	No Make default

Cancel

Update

Imagen 50: Asignando Perfil de Administración

Asignación de red al perfil de configuración

Para realizar completar el proceso de administración de dispositivos se debe indicar a cuál red se conectarán las iPad siguiendo de la siguiente forma:

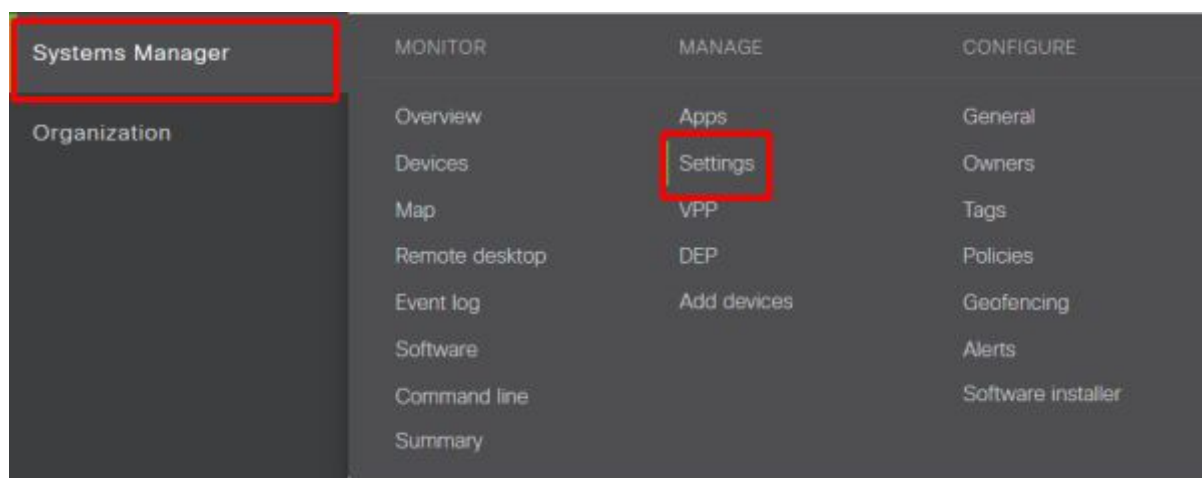


Imagen 51: Ingresar a Settings

Se selecciona el PERFIL- PRÉSTAMO previamente creado

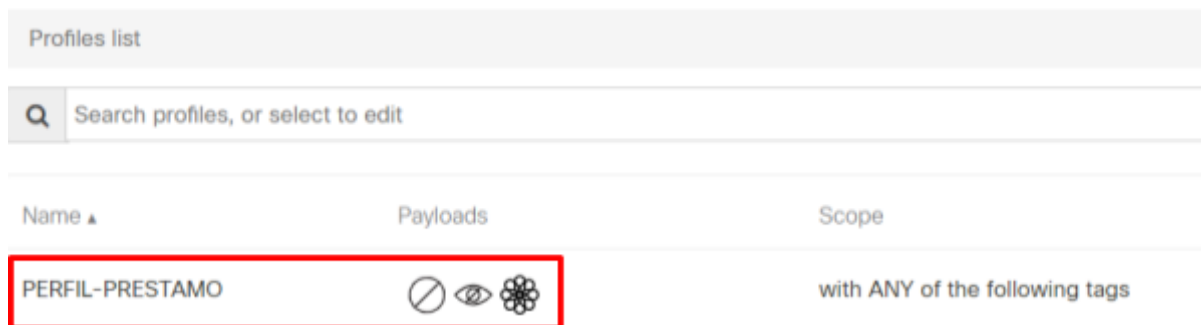


Imagen 52: Seleccionar perfil

Se ingresa a la configuración **WiFi Settings**

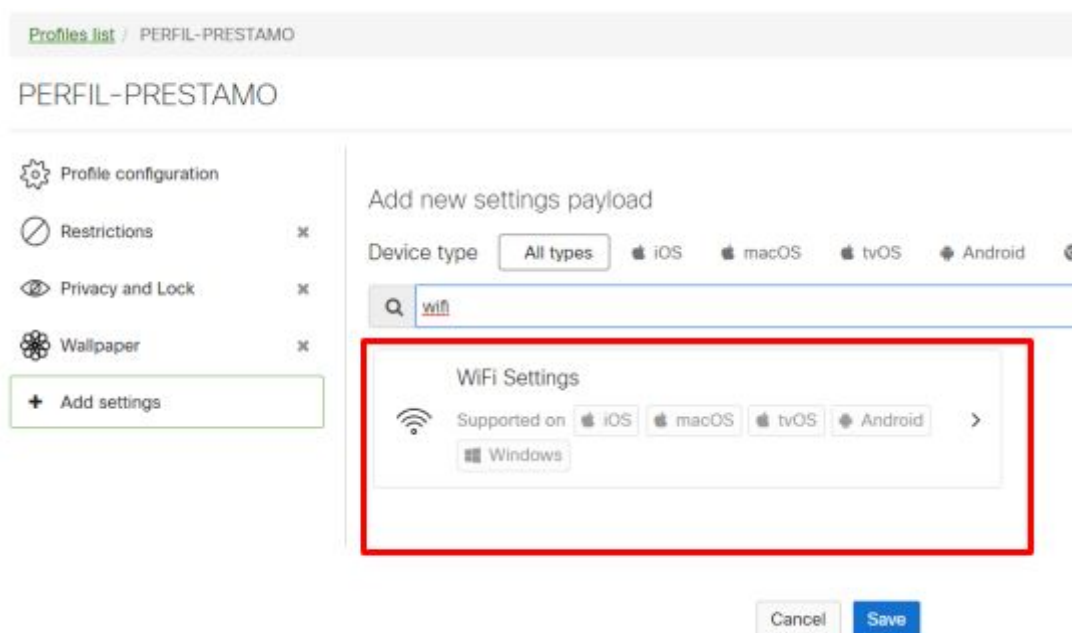


Imagen 53: Buscar la configuracion WiFi Settings

Se selecciona **Sentry** para ubicar la red que se tiene dedicada la entidad para el proyecto PC PUMA y se coloca en el apartado de Network dicha red y se llena, en caso de ser necesario, con los datos de dicha red. Al finalizar se guardan los cambios.

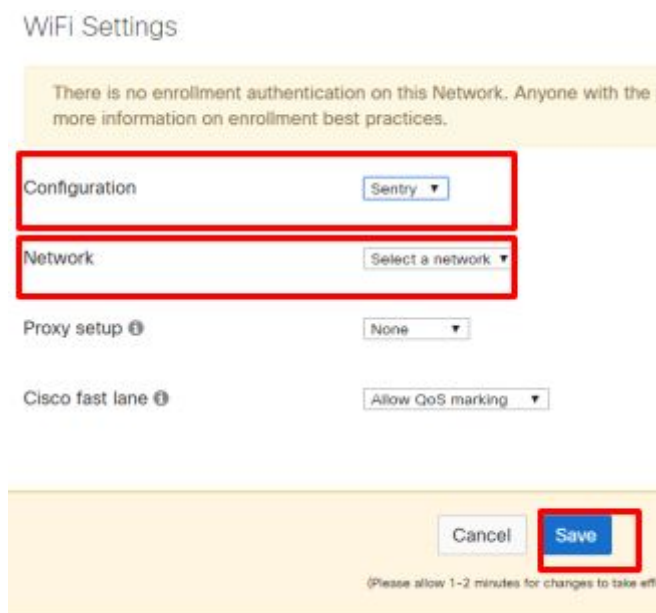


Imagen 54: Configuración de la red

Para tener control de las ipads deberá crearse una cuenta de correo electrónico de preferencia correo unam, que deberá emplearse únicamente para la administración de las ipads, dicha cuenta deberá asignarse como apple id en la siguiente página:

<https://appleid.apple.com/account#!&page=create>

Deberá asegurar los datos de la cuenta de correo electrónico (cuenta y password) y la contraseña asignada en la página de creación de apple id.

nombre@example.com
prestamopcpumaentidad@unam.mx

Este será tu nuevo Apple ID.

Contraseña
•••••

Confirmar contraseña
•••••

Imagen 55: Asignar la cuenta de correo creada como apple id



Al terminar de crear la cuenta de administración de las ipads y asignarla como apple id podemos proceder a encender las ipads, solo hasta este momento pueden encenderse las ipads para el proceso de enrolamiento y puesta a punto de este manual.

Encendido del iPad

Al encenderse el iPad deberá aparecer la siguiente imagen que indica que esa iPad está administrada remotamente por la **UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO**.

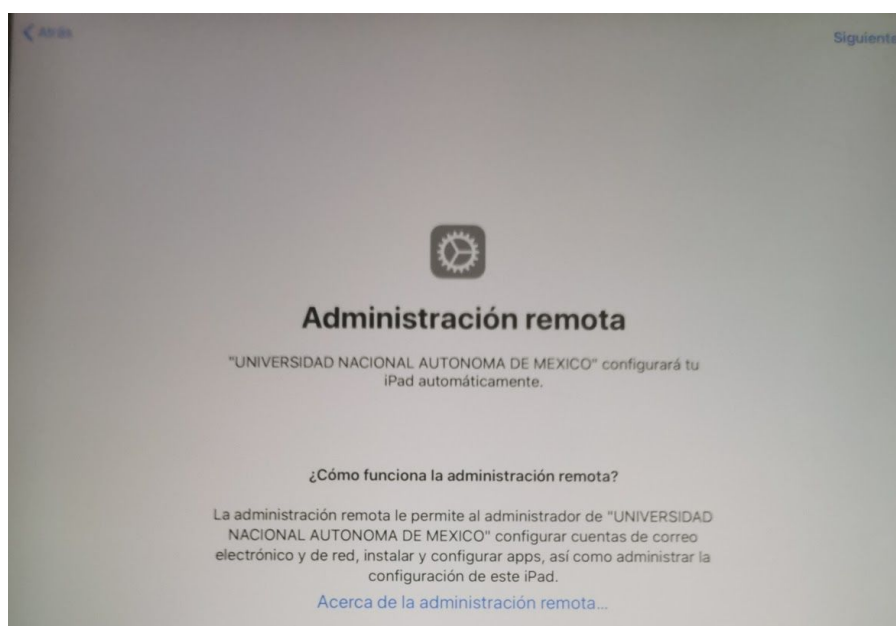


Imagen 56: Administración remota por la UNAM



Al terminal el inicio del dispositivo se pedirá que se ingrese un apple id, se deberá ingresar el apple id que se ha creado anteriormente y se podrá observar en el escritorio que las aplicaciones que se han indicado en el MDM comenzarán a descargarse. Ingresar a la aplicación **SM Meraki** y permitir la localización.

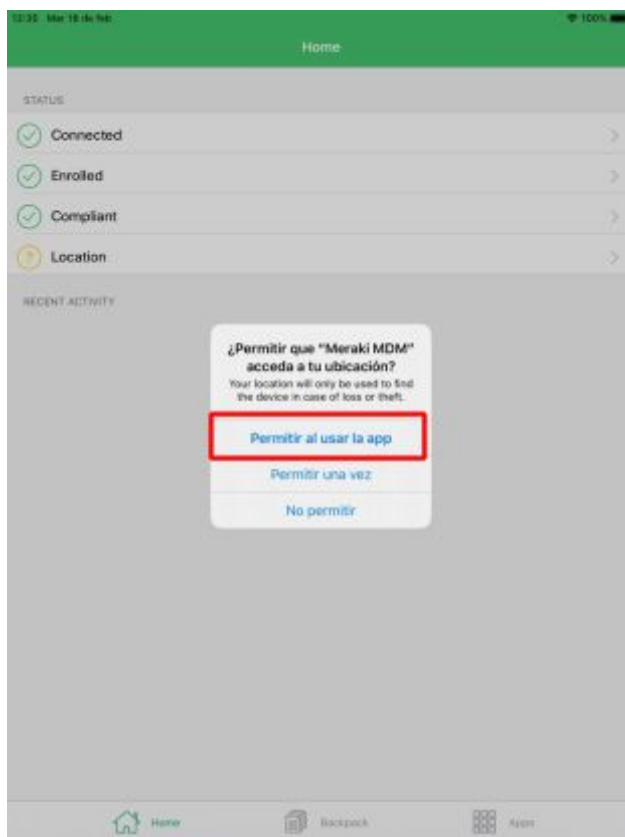


Imagen 57: Permitir ubicación



Enseguida deberá ingresarse a la configuración de la tablet y en la configuración de Meraki MDM



Imagen 58: Ingresar a configuración de Meraki MDM

En la configuración de SM Meraki marcar **Siempre** la ubicación

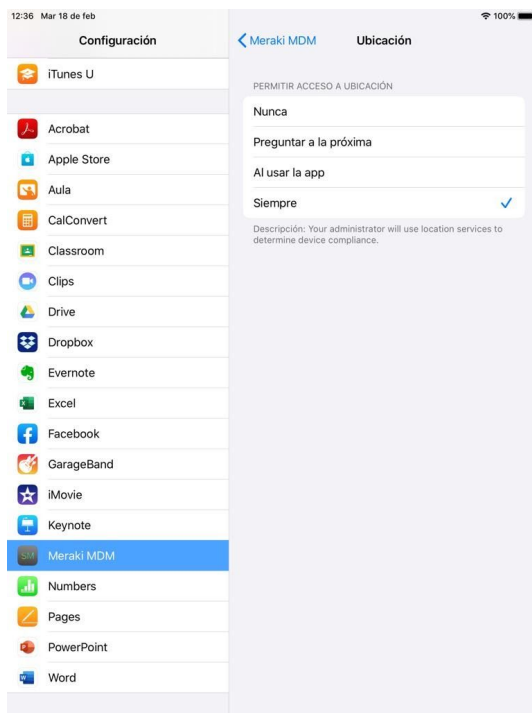


Imagen 59: Marcar Siempre



DISPOSITIVOS WINDOWS 10

Creación de cuenta para préstamo

Para utilizar un dispositivo Windows 10 administrado por el MDM de Meraki se deberá crear una cuenta que se se asignará a los dispositivos a ser enrolados; para Windows se recomienda que sea una cuenta Microsoft

Ejemplo:

prestamoentidad@hotmail.com

La cuenta de préstamo puede ser la misma para todos los dispositivos que tiene la entidad.

Enrolamiento

Para realizar el enrolamiento del dispositivo Windows 10 se deberá acceder al Dashboard de Cisco Meraki elegir la Organización a administrar, la red creada y el tag previamente creados.

Enseguida se selecciona el apartado **System Manager** y la sección **Manage** se da clic en **Add devices**

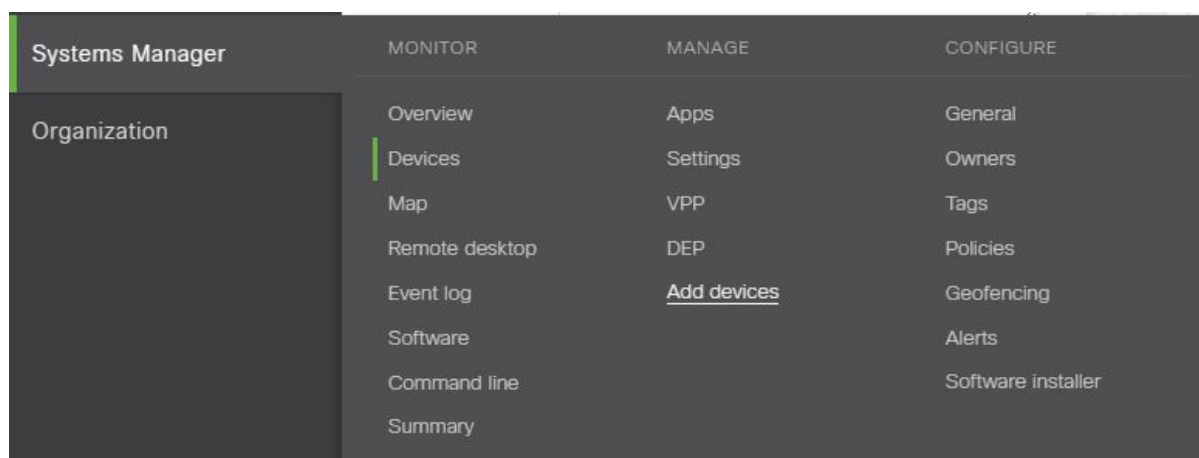


Imagen 60: Añadir dispositivos

Para añadir el dispositivo seleccionamos **Windows**

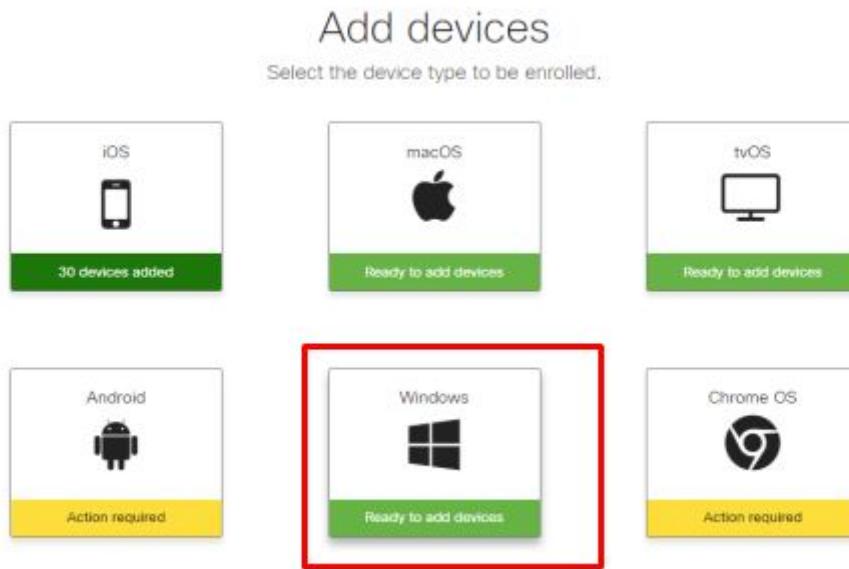


Imagen 61: Añadir dispositivos Windows

En la interfaz **Add Devices** vamos a colocar la cuenta previamente creada y damos clic en **Send**

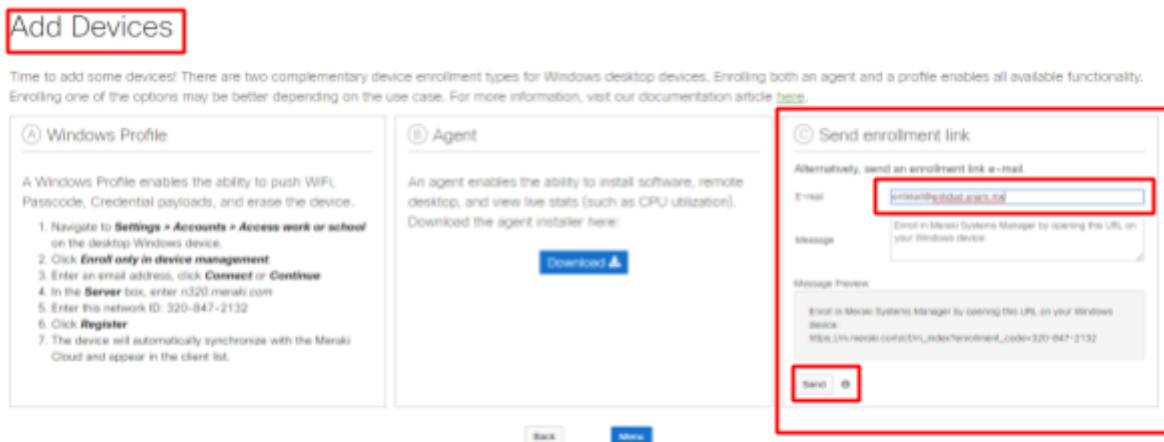


Imagen 62: Sección de envío de link de enrolamiento



Se deberá ingresar al correo pues el enlace de enrolamiento se ha enviado por correo a esa cuenta

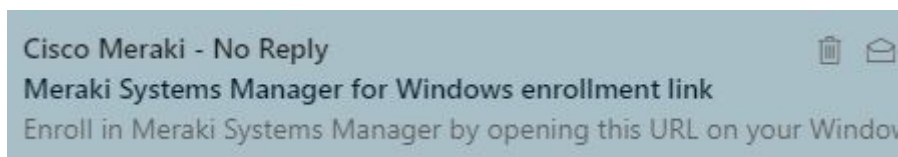


Imagen 63: Ejemplo de correo con link de enrolamiento

En el correo aparece el enlace que se presenta de la siguiente forma y damos clic al enlace

Enroll in Meraki Systems Manager by opening this URL on your Windows device:
https://m.meraki.com/?enrollment_code=320-

Imagen 64: Contenido de correo de enrolamiento

En el recuadro ya debe aparecer el **Network ID** y solo hay que dar clic en **Register**

Imagen 65: Registro de dispositivo Windows 10



En esta interfaz seleccionar **Download the Systems Manager Agent**



Imagen 66: Descarga de Systems Manager Agent

El registro se ha realizado y aparece una ventana para descargar el Agente de Meraki con un nombre de archivo de la forma: **MerakiSM-Agent-mdm_entidad.msi**, **no cierre la ventana del navegador hasta que termine de instalar el agente.**

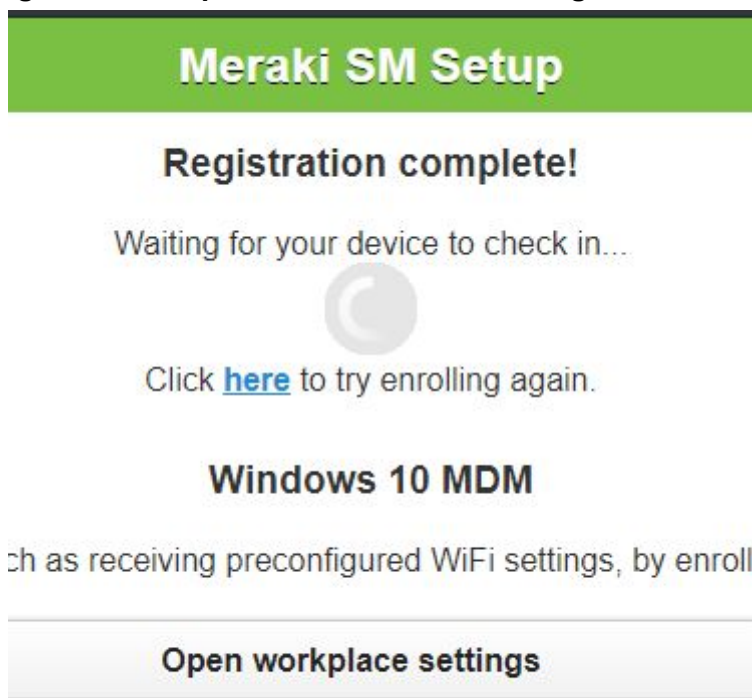


Imagen 67: Registro completo

Deberá descargarse el archivo e instalarse como se presenta en la siguiente sección.



Instalación de Agente

Acceder al directorio donde se se ha descargado el archivo del agente MerakiSM- Agent y dar doble clic en este para instalarlo

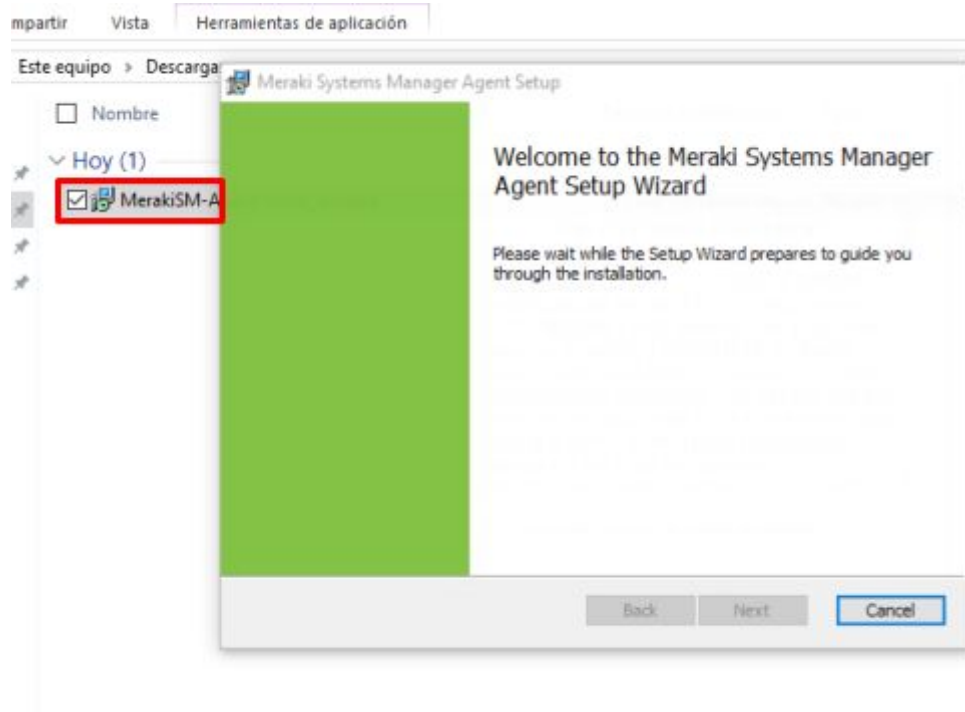


Imagen 68: Instalación del Agente

Hacer clic en la casilla de verificación **I accept the terms in the License Agreement** y dar clic en **Install**

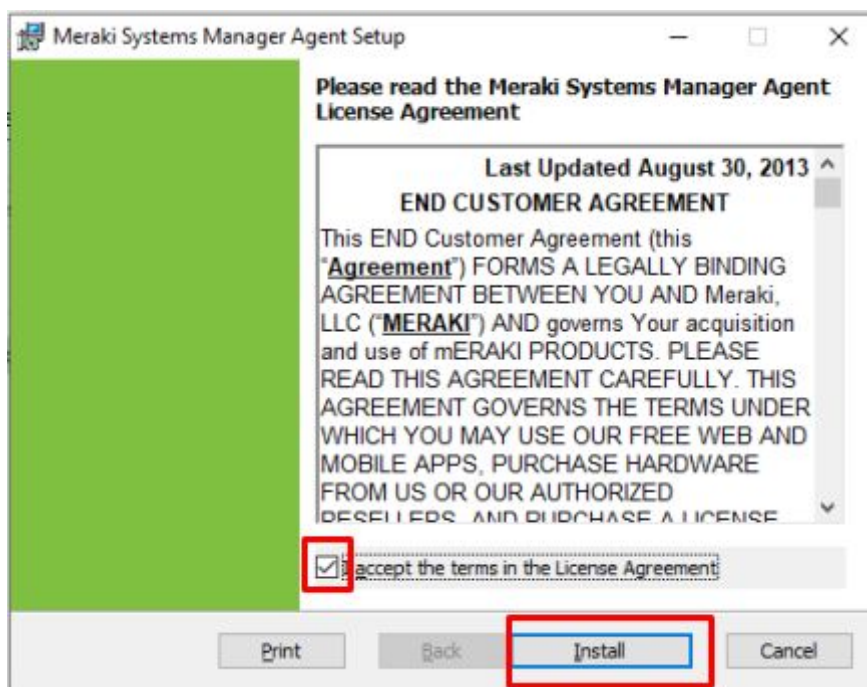


Imagen 69: Instalación del Agente



Aceptar la instalación si está activado el DAC de Windows y deberá aparecer la siguiente terminal, habrá que esperar a que se instale el agente para después verificar si ya aparece en el MDM de Meraki

```
C:\Program Files (x86)\Meraki\PCC Agent 1.0.98\m_agent_upgrade.exe
2020-02-25 13:35:13.483222 [028D1820]: main(): cannot use Windows temp; use GetTempPath
Agent registration
```

Imagen 70: Instalación del Agente

Verificación de enrolamiento

Para verificar que el dispositivo Windows 10 se ha enrolado correctamente se accede desde el dashboard de Cisco Meraki seleccionando la Organización, el tag y la red, enseguida se accede al apartado de **Systems Manager** y en la sección de **Monitor** seleccionamos **Devices**.

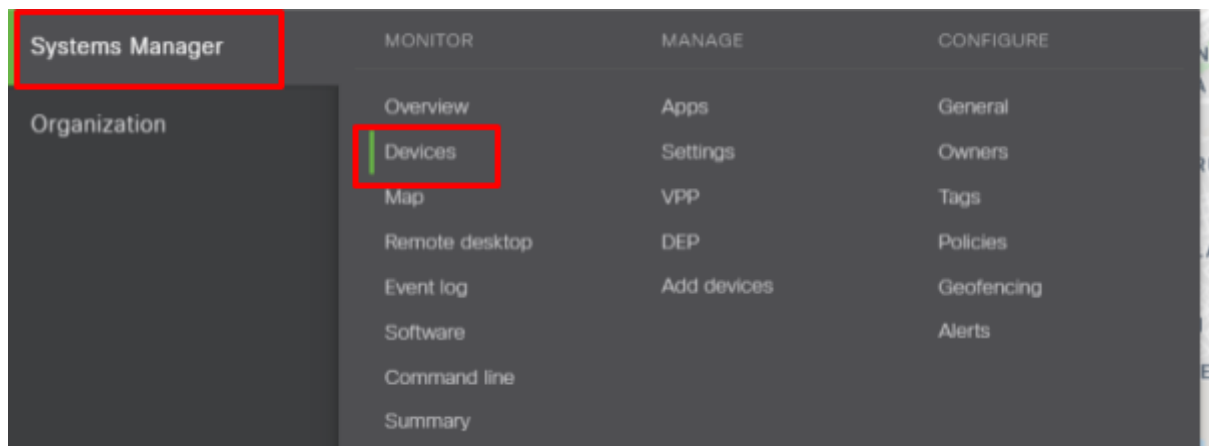


Imagen 71: Acceso a Dispositivos

En la interfaz deberá aparecer el dispositivo Windows 10 que recientemente enrolamos



Imagen 72: Dispositivo enrolado



DISPOSITIVOS CHROME OS

Debido a que pueden realizarse más tareas de administración, los dispositivos Chrome OS en el proyecto PC PUMA se enroлан directamente a la consola de Google (Google Management Console).

Enrolamiento de dispositivos

1. Para enroлар la Chromebook primero será necesario conectarse a internet
2. Enseguida aparecerá la pantalla de inicio de sesión de la chromebook para lo que será necesario utilizar las teclas Ctrl + Alt + E para registrar el dispositivo en la empresa.
3. Deberá ingresarse la cuenta de administración que hará que el dispositivo se agregue al inventario de la organización .

Puesta a punto de Chromebooks

Unidades organizativas

Las Unidades organizativas son entes a la cual se añaden políticas, restricciones y características propias para determinado ente, si se añade una unidad organizativa dentro de otra, la segunda heredará las características de la primera. De esta forma debe la entidad deberá plantear qué unidades organizativas implementar según sus necesidades dentro el proyecto PC PUMA.

Debido a que en el proyecto PC puma se manejan principalmente dos modalidades de préstamo se muestra para fines de ejemplo en este manual únicamente 2 unidades organizativas: Clases y Alumnos.

Para fines de ejemplo en este manual se realizará la unidad organizativa **Pruebas** que pretende crear de manera general una plantilla de guía sobre las políticas en la modalidad de préstamo a alumnos que deben implementarse en el proyecto PC PUMA..

Para ingresar a la consola de administración de google ingresamos al siguiente enlace:

<http://admin.google.com/>



Desde la consola de administración de Google ingresamos a la sección **Unidades Organizativas**

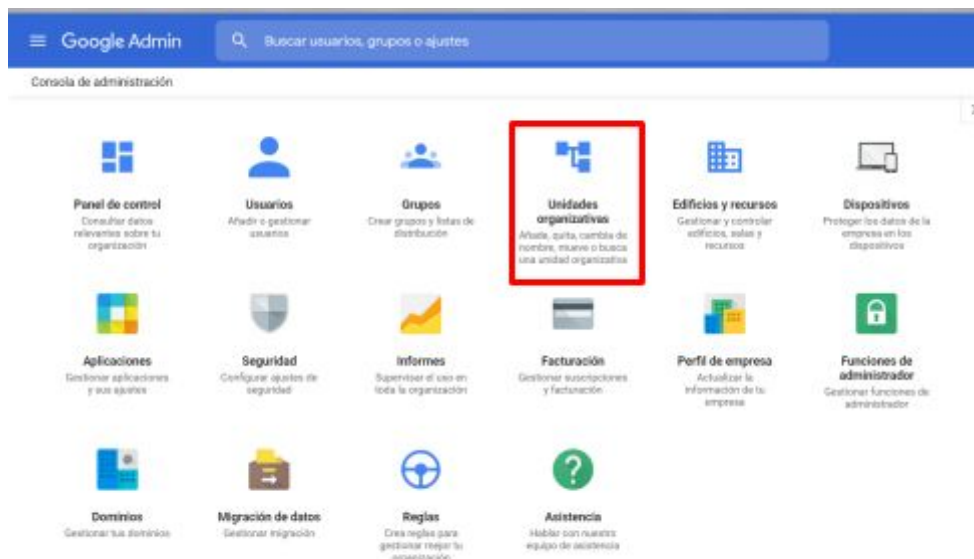


Imagen 73: Consola de Administración de Google

Se añade el nombre de la unidad organizativa y la descripción y se da clic en **Crear**

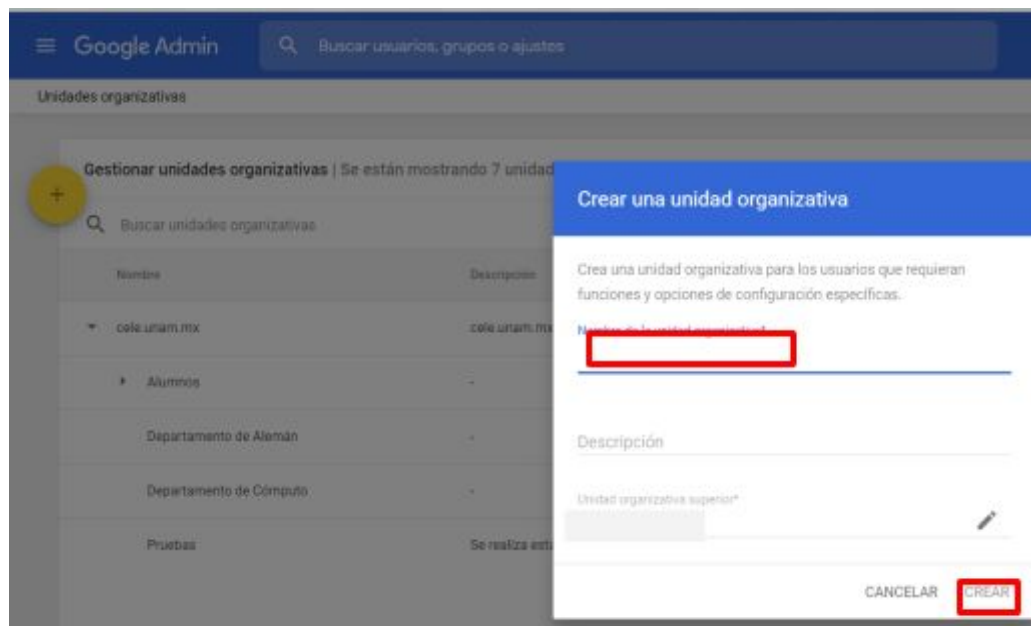


Imagen 74: Creación de unidad organizativa



Como se mencionó anteriormente se crea la unidad organizativa Pruebas como ejemplo para este manual :

Editar unidad organizativa

Pruebas

Nombre de la unidad organizativa*

Pruebas

Descripción

Se realiza esta unidad organizativa para realizar pruebas y establecer una plantilla de administración

CANCELAR ACTUALIZAR

Imagen 75: Nombre y descripción de la Unidad Organizativa

Es importante verificar que los cambios que necesiten realizarse se asignen en la unidad organizativa en específico o de ser necesario se asignen las políticas a todo el árbol de unidades organizativas que rige la entidad

Cada que se realice un cambio nuevo al implementar las políticas de Configuración de usuario y navegador, configuración de dispositivo, gestión de aplicaciones y redes siempre debe guardarse para que se apliquen los cambios en los dispositivos.

Creación de Usuario para administración

Para la administración de las chromebooks es necesario crear un usuario que se ingresará a cada chromebook para poder propagar las políticas y restricciones implementadas, para ello es necesario ingresar a la consola de google y acceder a la sección de **Usuarios**

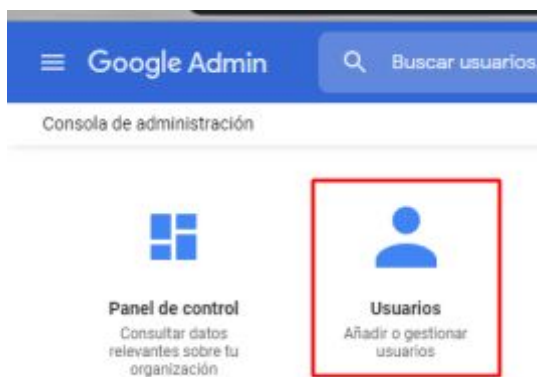


Imagen 76: Sección usuario en la consola de google

Se selecciona la Unidad organizativa a la que se desea agregar ese Usuario para poder ingresarlo directamente en las chromebooks para poder ser un usuario al cual se va a administrar

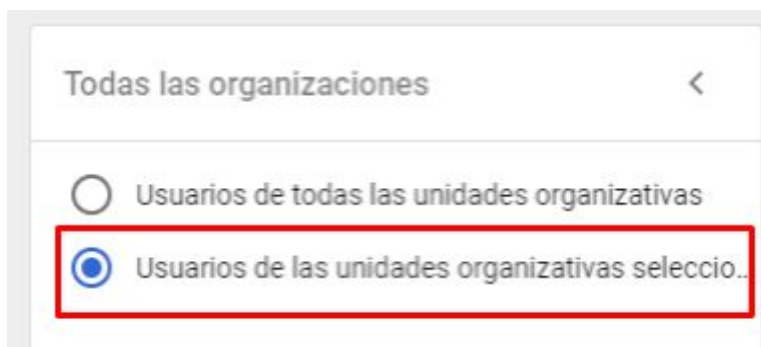


Imagen 77: Selección de Unidad organizativa a la que tiene acceso el usuario a crear

Seleccionar **Añadir usuario nuevo**



Imagen 78: Añadir usuario



Después de llenar los campos obligatorios dar clic en **Añadir usuario nuevo**

Imagen 79: Añadir usuario

	Nombre	Correo electrónico	Estado	Último acceso	Uso del correo elect.
<input type="checkbox"/>	Préstamo	prestamo@unam.mx	Activo (añadido recientemente)	Hace 1 minuto	0 GB

Imagen 80: Usuario para administración de dispositivos de préstamo

Recuerde guardar el correo electrónico y la contraseña del usuario que se emplea para la administración de las chromebooks.

En adelante se recomienda ingresar a una de las chromebooks y firmarse con el correo y contraseña creados en el paso anterior para ver reflejados los cambios en los dispositivos



y establecer a partir de la siguiente guía las políticas en una unidad organizativa establecida por la entidad desde la consola de google.

Configuración de usuario y navegador

Para añadir configuraciones que administren las políticas para los usuarios desde la consola de google se ingresa a **Dispositivos**

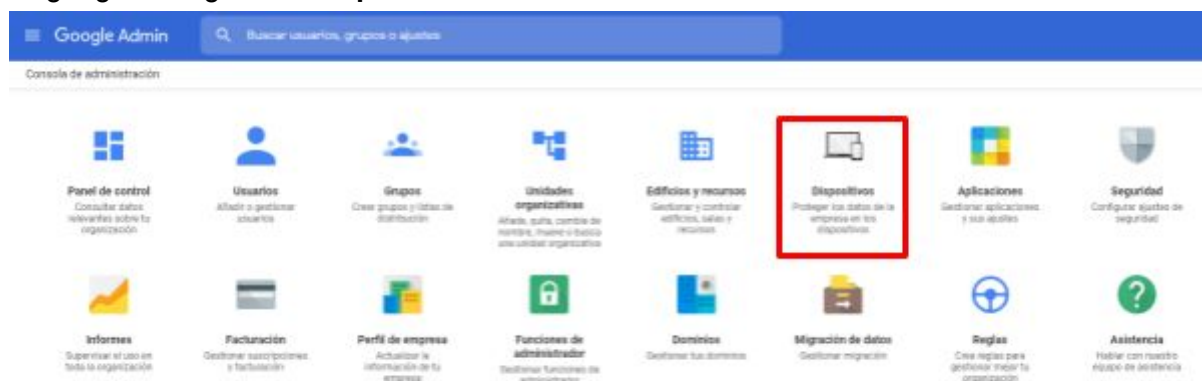


Imagen 81: Sección Dispositivos

Se ingresa a **Administración de dispositivos** en el menú lateral

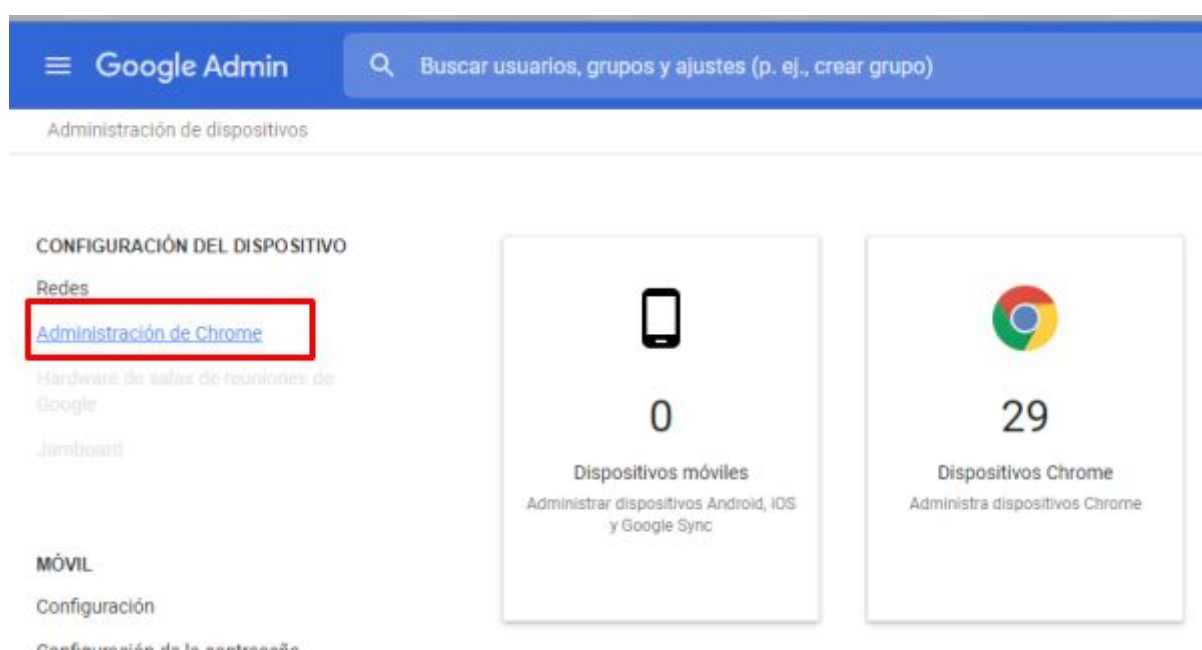




Imagen 82: Menú lateral: Administración de Chrome

Entrar a la sección de **Configuración de usuario y de navegador**

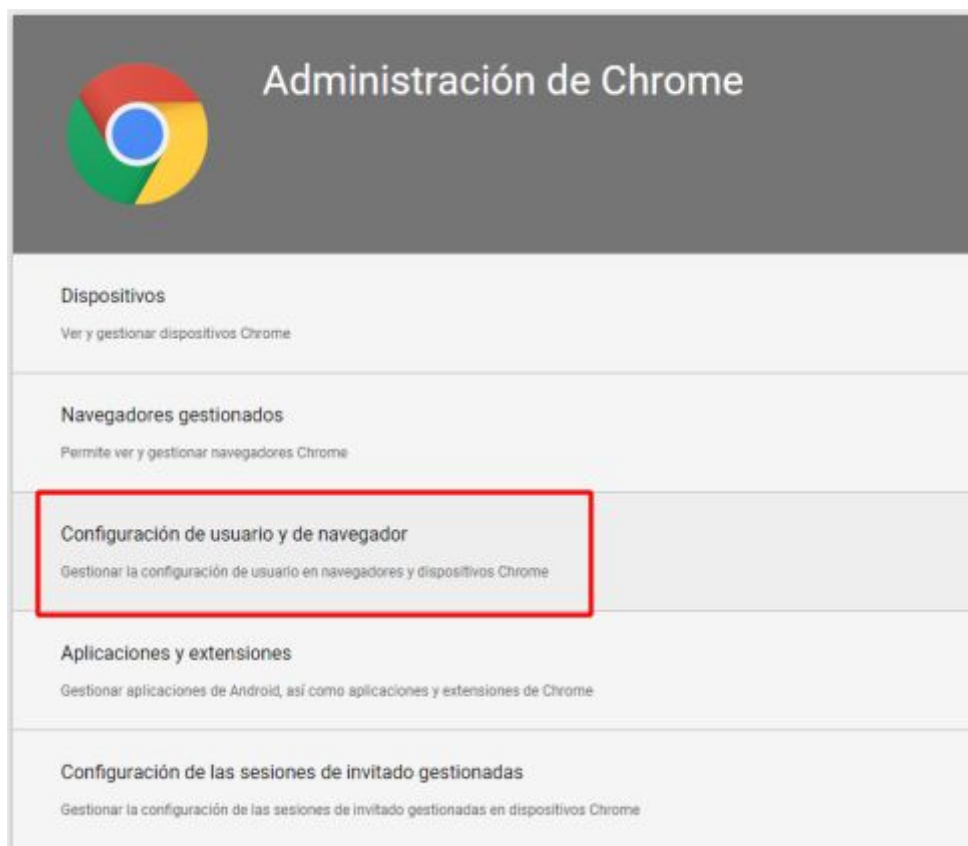


Imagen 83: Configuración de usuario y de navegador

Se debe elegir la **UNIDAD ORGANIZATIVA** a la que queremos aplicar los cambios, para fines de muestra se asignan en este manual los cambios a la **UNIDAD ORGANIZATIVA Pruebas**

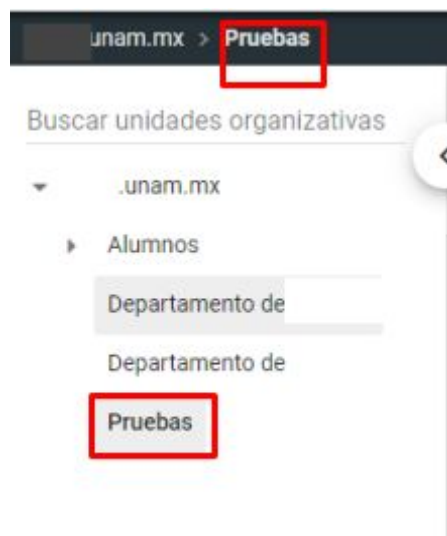


Imagen 84: Pruebas

En la sección **General** se añade un fondo de pantalla que será el que se mostrará en el escritorio de la chromebook

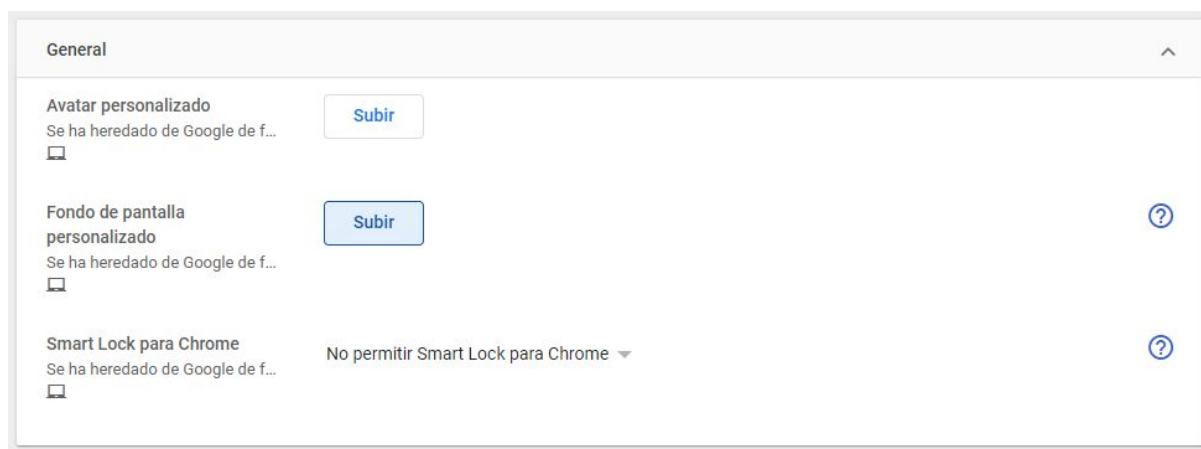


Imagen 85: Sección General - Wallpaper personalizado

En la sección **Configuración de inicio de sesión** establecer las siguientes políticas

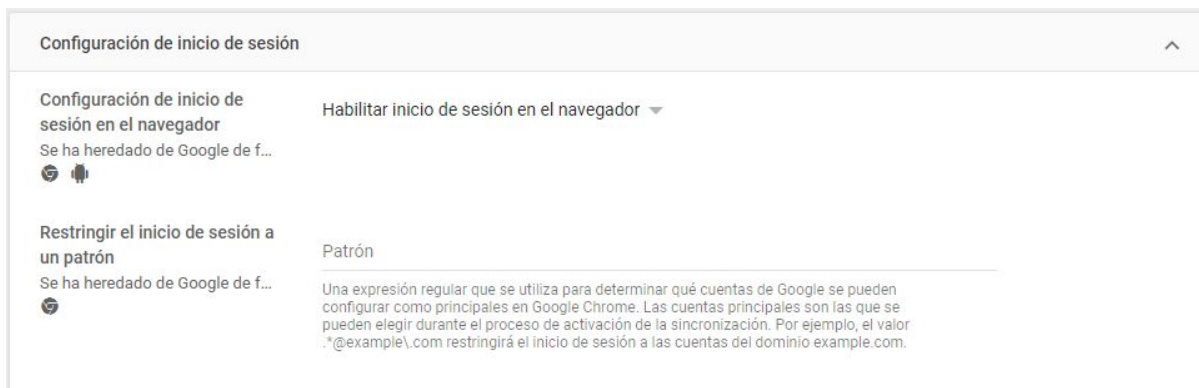


Imagen 86: Configuración de inicio de sesión

Sección Móvil

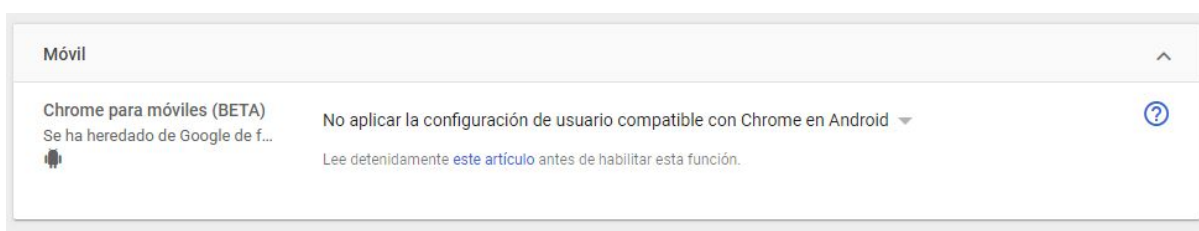


Imagen 87: Móvil

Aplicar a la configuración **Controles de registro** de la siguiente forma:

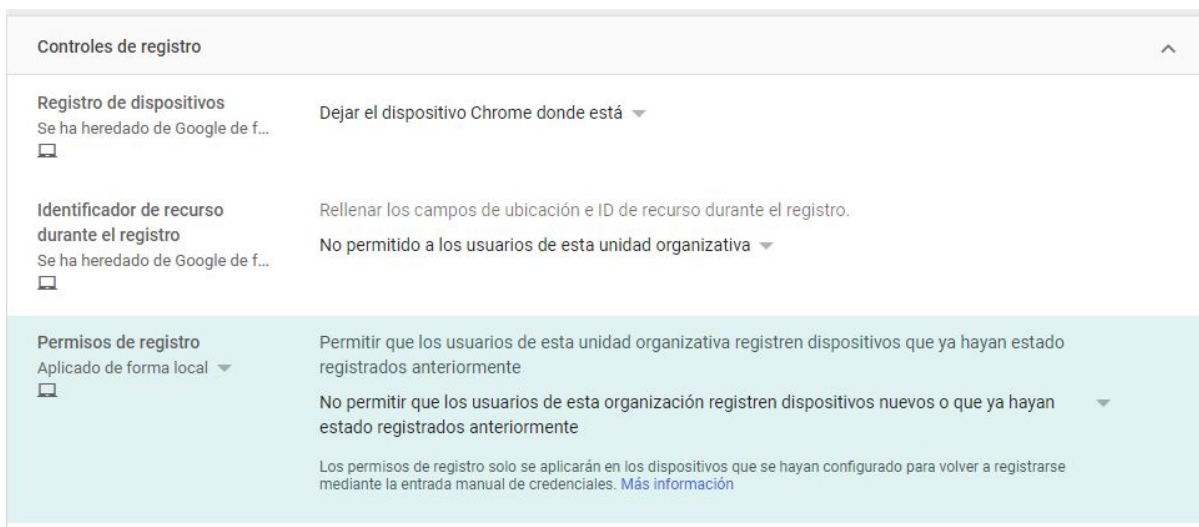


Imagen 88: Controles de registro

Para la configuración de **Aplicaciones y extensiones** se aplica la siguiente política

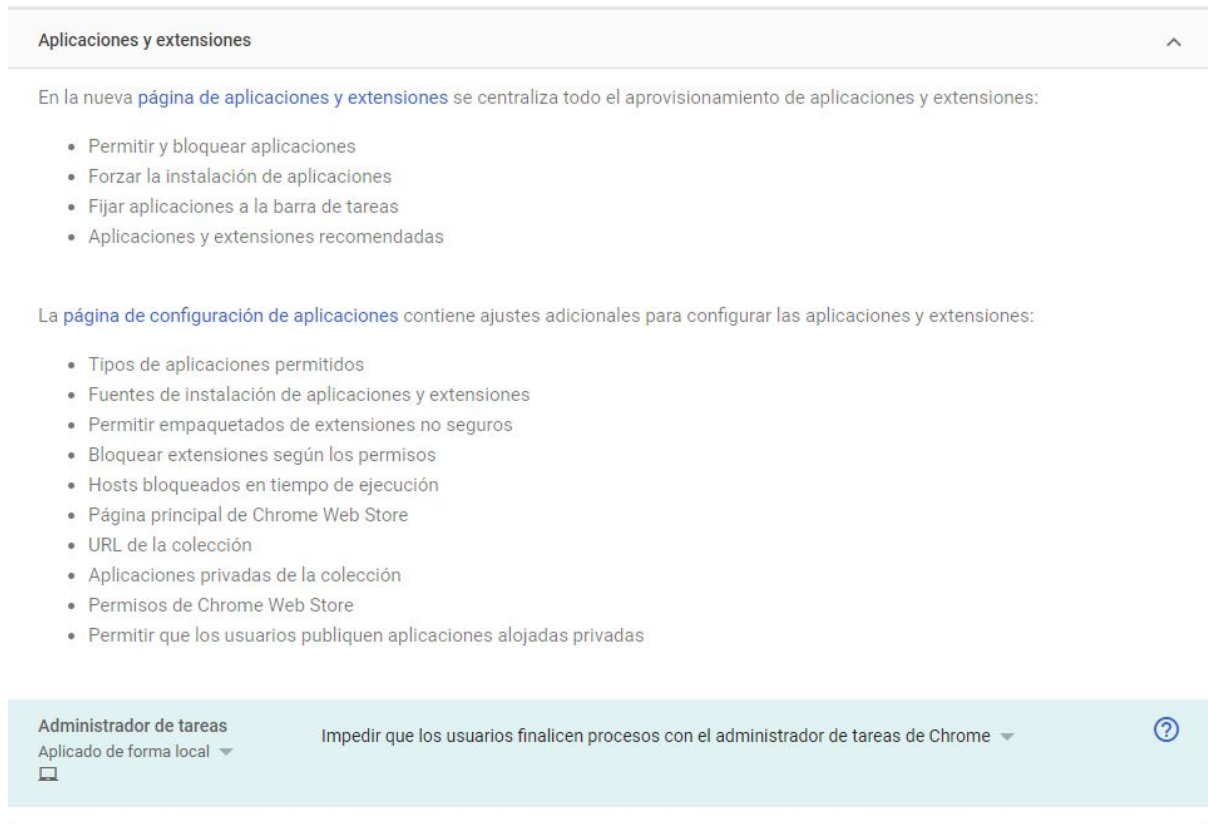


Imagen 89:Aplicaciones y extensiones

En la configuración **Aislamiento de sitio web** se deberán agregar sitios web que la entidad considere



Imagen 90: Aislamiento de sitios web



En la sección de **Seguridad** establecer las siguientes políticas:

Seguridad	
Gestor de contraseñas Se ha heredado de Google de f... 	Permitir que el usuario decida ▾
Bloquear pantalla Se ha heredado de Google de f... 	Permitir el bloqueo de la pantalla ▾
Desbloqueo rápido Se ha heredado de Google de f... 	<input type="checkbox"/> PIN <input type="checkbox"/> Huella digital
Configuración de inactividad Se ha heredado de Google de f... 	Tiempo de inactividad en minutos <hr/> Si quieres aplicar la opción predeterminada del sistema, no indiques ningún valor. Acción al entrar en estado ausente Entrar en suspensión ▾ Acción al cerrar la tapa Entrar en suspensión ▾ Bloquear pantalla al entrar en suspensión Permitir que el usuario elija la configuración ▾
Modo de incógnito Aplicado de forma local ▾ 	No permitir el modo de incógnito ▾
Historial del navegador Se ha heredado de Google de f... 	Guardar siempre el historial del navegador ▾
Borrar el historial de navegación Aplicado de forma local ▾ 	No permitir que se borre el historial en el menú de configuración ▾
Forzar modo efímero Aplicado de forma local ▾ 	Borrar datos locales al cerrar el navegador Borrar todos los datos de usuario locales ▾
Comprobaciones de revocación online Se ha heredado de Google de f... 	Comprobaciones de OCSP/CRL online No realizar comprobaciones de OCSP/CRL online ▾
Geolocalización Aplicado de forma local ▾ 	Permitir que los sitios web detecten la geolocalización de los usuarios ▾
Frecuencia de acceso online mediante inicio de sesión único Se ha heredado de Google de f... 	Forzar flujo de inicio de sesión online para las cuentas de inicio de sesión único basado en SAML Cada 2 semanas ▾ Configura el inicio de sesión único (SSO) en G Suite antes de empezar a utilizar esta política



UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
SECRETARÍA DE DESARROLLO INSTITUCIONAL
Manual de enrolamiento MDM y puesta a punto de dispositivos v.1.4

Inicio de sesión único Se ha heredado de Google de f... 	Inicio de sesión único basado en SAML para dispositivos Chrome OS Inhabilitar inicio de sesión único basado en SAML en dispositivos Chrome ▼ Configura el inicio de sesión único (SSO) en G Suite antes de empezar a utilizar esta política
Paquete de cifrado RC4 en TLS Se ha heredado de Google de f... 	Inhabilitar RC4 ▼
Clientes de acceso remoto Se ha heredado de Google de f... 	Acceso remoto según dominio de cliente establecido por el host <hr/> <p>Configura los nombres de dominio requeridos para los clientes de acceso remoto (un dominio en cada línea). En Chrome 59 y versiones anteriores solo se admite un nombre de dominio, por lo que se utilizará el primer dominio de la lista.</p>
Certificados de anclajes de confianza locales Se ha heredado de Google de f... 	SHA-1 de anclajes locales Seguir la programación de desactivación de SHA-1 anunciada de forma pública ▼ <hr/> <p>Controla si se permiten los certificados firmados por SHA-1 emitidos por los anclajes de confianza locales. Si se ha habilitado este ajuste, Chrome permitirá los certificados firmados de SHA-1 siempre que se validen y se vinculen correctamente con certificados de CA instalados de forma local. Nota: Esta opción dejará de estar disponible el 1 de enero del 2019.</p> <p>Opción alternativa para el nombre común de los anclajes locales</p> <p>Bloquear ▼</p> <p>Controla si deben permitirse o bloquearse los certificados emitidos por los anclajes de confianza locales que no tienen la extensión subjectAlternativeName. Si se ha habilitado este ajuste, Chrome usará el commonName del certificado de un servidor para que coincida con un nombre de host si el certificado no tiene una extensión subjectAlternativeName, siempre que se valide y se vincule satisfactoriamente con certificados de CA instalados de forma local. Ten en cuenta que esto no se recomienda, ya que se puede omitir la extensión nameConstraints que restringe los nombres de host para los que un certificado determinado puede recibir autorización.</p> <p>Infraestructura de PKI antigua de Symantec Corporation</p>
	Bloquear ▼ <hr/> <p>Autoriza la aprobación de los certificados emitidos por la infraestructura PKI antigua de Symantec Corporation si se han validado con algún otro método y están vinculados a un certificado de CA reconocido. Ten en cuenta que, en los sistemas que no utilizan Chrome OS, esta política se aplicará si el sistema operativo aún reconoce los certificados de la infraestructura antigua de Symantec. Si la gestión de estos certificados se modifica mediante una actualización del sistema operativo (SO), esta política dejará de tener efecto. Además, esta política es una solución temporal cuyo fin es ofrecer a las empresas más tiempo para abandonar los certificados antiguos de Symantec y dejará de estar disponible en torno al 1 de enero del 2019.</p>
Lista blanca de URL de transparencia en los certificados Se ha heredado de Google de f... 	Lista blanca de URL de transparencia en los certificados <hr/> <p>La transparencia en los certificados no será obligatoria en las URL indicadas. Introduce una URL por línea. Más información</p>
Lista blanca de transparencia en los certificados de CA Se ha heredado de Google de f... 	Lista blanca de transparencia en los certificados de CA <hr/> <p>Los hashes subjectPublicKeyInfo indicados estarán exentos de la aplicación de transparencia en los certificados. Estos hashes deben indicarse en un formato específico. Introduce un hash por línea. Más información</p>
Lista blanca de transparencia en los certificados de CA antiguas Se ha heredado de Google de f... 	Lista blanca de transparencia en los certificados de CA antiguas <hr/> <p>Los hashes subjectPublicKeyInfo indicados estarán exentos de la aplicación de transparencia en los certificados. Estos hashes deben indicarse en un formato específico y deben coincidir con una autoridad de certificación antigua reconocida. Introduce un hash por línea. Más información</p>
Programador de tareas de la CPU Aplicado de forma local ▼ 	Controla si la tecnología Hyper-Threading de Intel está inhabilitada o si se pueden usar todos los núcleos sin restricciones. Optimizar para aumentar el rendimiento. ▼



Habilitar la integridad de
código del renderizador

Se ha heredado de Google de f...



Integridad de código del renderizador habilitada ▼

Habilitar la detección de
filtraciones de datos para las
credenciales introducidas

Se ha heredado de Google de f...



Habilitar la detección de filtraciones de datos para las credenciales introducidas ▼

Configuración de sesión



Mostrar botón de cerrar
sesión en la bandeja

Se ha heredado de Google de f...



No mostrar el botón de cerrar sesión en la bandeja ▼

Imagen 91: Seguridad
En la sección de **Red** establecer las siguientes políticas:



Red

Modo proxy

Aplicado de forma local

Esquemas de autenticación admitidos

Se ha heredado de Google de f...

No utilizar nunca un servidor proxy

Esquemas de autenticación admitidos

☒ Basic

☒ Resumen

☒ NTLM

☒ Negociar

Especifica los esquemas de autenticación HTTP compatibles con Google Chrome. La configuración predeterminada utiliza los cuatro esquemas.

División de registros de SSL

Se ha heredado de Google de f...

Proxy de compresión de datos

Se ha heredado de Google de f...

Puertos WebRTC UDP

Se ha heredado de Google de f...

Protocolo QUIC

Se ha heredado de Google de f...

Versión antigua del CORS

Se ha heredado de Google de f...

Medidas de atenuación del uso compartido de recursos de origen cruzado (CORS)

Se ha heredado de Google de f...

Habilitar

Versión antigua

Versión antigua inhabilitada

Se prefiere la implementación de CORS antigua a la nueva. Esta opción desaparecerá con la versión de Chrome 81.

Permitir que el usuario decida

Permite que WebRTC elija cualquier puerto UDP (1024-65535).

Habilitar la división de registros de SSL

Predeterminado (no se aplican atenuaciones)

Habilita las atenuaciones del CORS en las extensiones de Chrome. No se aplica si el dispositivo está usando la versión antigua del COR.

Imagen 92: RED



Aplicaciones Android

Algunos ajustes de gestión de las aplicaciones Android para usuarios de Chrome OS se han trasladado a la nueva [página de aplicaciones y extensiones](#), por ejemplo:

• Aplicaciones Android en dispositivos Chrome

• Informes de Android para usuarios y dispositivos

Controlar el servicio de copia de seguridad y restauración de Android

Se ha heredado de Google de f...

Servicios de ubicación de Google

Se ha heredado de Google de f...

Gestión de cuentas

Se ha heredado de Google de f...

Sincronización de certificados

Se ha heredado de Google de f...

Puedes restaurar los datos de usuario y cambiar de dispositivo fácilmente y en cualquier momento. En la copia de seguridad del usuario se incluyen los datos de la aplicación.

Función de copia de seguridad y restauración inhabilitada

Por datos de la aplicación se entiende cualquier dato que una aplicación haya guardado (en función de los ajustes del desarrollador), incluidos los datos potencialmente sensibles como los contactos, los mensajes y las fotos. Los datos de la copia de seguridad no se contabilizan en la cuota de almacenamiento de Drive del usuario.

No permitir a las aplicaciones Android utilizar los servicios de ubicación en Chrome OS

Google puede recoger datos de ubicación cada cierto tiempo y usarlos de forma anónima para ofrecer una ubicación más precisa y mejorar los servicios basados en ella. El servicio de ubicación de Google usa fuentes como redes Wi-Fi, redes móviles y sensores para estimar la ubicación de un dispositivo. Este servicio está activado si los ajustes de ubicación de un dispositivo también lo están.

Impedir que los usuarios añadan estos tipos de cuenta:

☐ Cuenta de Google

Advertencia: Esta política ha quedado obsoleta; solo se aplica a los dispositivos con Chrome OS M75 y versiones anteriores, y a los dispositivos con Chrome OS M76 en los que todavía no se ha activado Google Account Manager.

Sincronizar los certificados de Google Chrome OS con las aplicaciones de Android.

Inhabilitar el uso de certificados de CA de Chrome OS en aplicaciones de Android

Imagen 93: Seguridad

En la sección de **Inicio** se deberán aplicar las siguientes políticas donde la página de inicio puede ser una que la entidad considere adecuada.

Inicio

Botón de inicio

Aplicado de forma local

No mostrar nunca el botón de inicio

Página principal

Aplicado de forma local

La página de inicio será siempre la URL que se indica más abajo

URL de página principal

unam.mx

Páginas que deben cargarse al inicio

Aplicado de forma local

[Páginas de inicio](#)

unam.mx

Coloca cada URL en una línea diferente. Por ejemplo:
example.org
https://example.com

Imagen 94: Inicio



En la sección **Contenido** se deben aplicar las siguientes políticas

Contenido	
Búsqueda Segura y modo restringido Aplicado de forma local ▼ 	Utilizar Búsqueda Segura en las consultas de la Búsqueda de Google No utilizar Búsqueda Segura en las consultas de la Búsqueda de Google ▼ Modo restringido en YouTube Aplicar como mínimo el modo restringido moderado en YouTube ▼
Captura de pantalla Se ha heredado de Google de f... 	Permitir que los usuarios hagan capturas de pantalla ▼
Certificados de cliente Se ha heredado de Google de f... 	Selección automática en estos sitios web Si un sitio web que coincide con un patrón indicado anteriormente solicita un certificado de cliente, Chrome seleccionará uno de forma automática. Puedes encontrar más información y valores de ejemplo en este artículo del Centro de Ayuda . Coloca un patrón por línea.
Confirmación de llaves de seguridad Se ha heredado de Google de f... 	Introducir URL o dominio Especifica los dominios y las URL con los que no se muestran mensajes cuando se solicitan certificados de confirmación a las llaves de seguridad. Además, se enviará un indicador a la llave de seguridad que indique el posible uso de una confirmación individual. Sin este ajuste, los usuarios recibirán un mensaje en Chrome 65 o versiones superiores cuando los sitios soliciten confirmación de llaves de seguridad. Las URL (como "https://example.com/alguna/ruta") se consignarán solo como AppIDs U2F. Por su parte, los dominios (como "example.com") se consignarán solo como IDs de usuario de confianza de WebAuthn. Por lo tanto, si quieres abarcar las API de U2F y de WebAuthn para un sitio web concreto, se deberán incluir el dominio y la URL de AppID. Solo un patrón por línea.
Cookies Se ha heredado de Google de f... 	Configuración predeterminada de cookies Permitir que el usuario decida ▼ Permite decidir si los sitios web pueden definir datos locales. Habilitar cookies en patrones de URL Coloca un patrón en cada línea. Bloquear cookies en patrones de URL Coloca un patrón en cada línea. Permitir cookies de solo una sesión en los patrones de URL Coloca un patrón en cada línea.
Bloqueo de cookies de terceros Se ha heredado de Google de f... 	Permitir que el usuario decida ▼



UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
SECRETARÍA DE DESARROLLO INSTITUCIONAL
Manual de enrolamiento MDM y puesta a punto de dispositivos v.1.4

Comportamiento antiguo
predeterminado de las
cookies con SameSite
Se ha heredado de Google de f...



Utilizar el comportamiento predeterminado de las cookies con SameSite en todos los sitios web ▼

Comportamiento antiguo de
las cookies con SameSite en
cada sitio web
Se ha heredado de Google de f...



Restaurar el comportamiento antiguo de las cookies con SameSite en estos sitios web

Introduce un sitio web por línea. Añade el prefijo [*] al dominio para incluir todos los subdominios.

Imágenes
Se ha heredado de Google de f...



Permitir que el usuario decida ▼

Mostrar imágenes en estos sitios web

Coloca un patrón en cada línea.

Bloquear imágenes en estos sitios web

Coloca un patrón en cada línea.

JavaScript
Se ha heredado de Google de f...



Permitir que el usuario decida ▼

Permitir que estos sitios web ejecuten JavaScript

Coloca un patrón en cada línea.

Bloquear JavaScript en estos sitios web

Coloca un patrón en cada línea.

Notificaciones
Se ha heredado de Google de f...



Permitir que el usuario decida ▼

Permitir que estos sitios web muestren notificaciones

Coloca un patrón en cada línea.

Bloquear notificaciones en estos sitios web

Coloca un patrón en cada línea.

Complementos
Se ha heredado de Google de f...



Permitir que el usuario decida ▼

Permitir complementos en estos sitios

Coloca un patrón en cada línea.

Bloquear complementos en estos sitios

Coloca un patrón en cada línea.





UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
SECRETARÍA DE DESARROLLO INSTITUCIONAL
Manual de enrolamiento MDM y puesta a punto de dispositivos v.1.4

Complementos habilitados e inhabilitados

Se ha heredado de Google de f...



Complementos habilitados

Introduce los nombres o patrones de los complementos que quieras habilitar siempre. Por ejemplo, para habilitar cualquier complemento que incluya "Gears", introduce "Gears". Coloca un patrón por línea. Se distingue entre mayúsculas y minúsculas.

Complementos inhabilitados

Introduce los nombres o patrones de los complementos que quieras inhabilitar siempre. Coloca un patrón por línea. Se distingue entre mayúsculas y minúsculas.

Excepciones para complementos inhabilitados

Permite a los usuarios habilitar o inhabilitar los complementos que se muestran aquí, incluso si también coinciden con una o varias entradas en la lista de complementos inhabilitados. Coloca un patrón en cada línea.

Buscador de complementos

Aplicado de forma local ▼



Inhabilitar la búsqueda automática y la instalación de complementos que faltan ▼

Autorización para usar complementos

Se ha heredado de Google de f...



Solicitar el permiso del usuario antes de ejecutar complementos que requieren autorización ▼

Complementos no actualizados

Se ha heredado de Google de f...



Solicitar permiso al usuario para ejecutar complementos no actualizados ▼

Ventanas emergentes

Se ha heredado de Google de f...



Permitir que el usuario decida ▼

Sincronización de Google Drive

Se ha heredado de Google de f...



Permitir que el usuario decida ▼

Sincronización de Google Drive a través de la red de datos móviles

Aplicado de forma local ▼



Sincronizar datos con Google Drive a través de conexiones de datos móviles

Inhabilitar la sincronización de Google Drive a través de conexiones de datos móviles ▼

Enviar

Aplicado de forma local ▼



Permitir a los usuarios enviar contenido desde Chrome

Permitir que los usuarios envíen contenido ▼

No mostrar el icono Enviar en la barra de herramientas de forma predeterminada, pero dejar que los usuarios elijan ▼

Tratamiento estricto del contenido mixto

Se ha heredado de Google de f...



Tratar de forma estricta el contenido mixto ▼

Si se habilita esta política, el contenido mixto se actualiza automáticamente a HTTPS (es decir, la URL se reformula con el patrón HTTPS y no hay respaldo si el recurso no está disponible a través de HTTPS) y en la barra de direcciones se advierte de que el contenido mixto con imágenes no es seguro.

Controlar el uso de las excepciones de contenido no seguro

Se ha heredado de Google de f...



Impedir que los sitios web carguen contenido mixto bloqueable ▼





UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
SECRETARÍA DE DESARROLLO INSTITUCIONAL
Manual de enrolamiento MDM y puesta a punto de dispositivos v.1.4

Permitir el contenido no seguro en estos sitios web
Se ha heredado de Google de f...

Patrones de URL que quieres permitir (uno por línea)

Bloquear el contenido no seguro en estos sitios web
Se ha heredado de Google de f...

Patrones de URL que quieres bloquear (uno por línea)

Volver a habilitar la API Web Components v0 en versiones anteriores a Chrome 84.
Se ha heredado de Google de f...

No volver a habilitar la API Web Components v0

La API Web Components v0 se desactivó en 2018. Esta política permite volver a habilitarla en versiones anteriores a Chrome 84 (a partir de esta versión ya no es posible hacerlo).

Solicitudes XHR síncronas al abandonar la página
Se ha heredado de Google de f...

Bloquear solicitudes XHR síncronas durante la descarga de la página

Nota: Esta política se eliminará en Chrome 88.

Imagen 95: Contenido

En la sección de **Impresión** se deberán aplicar las siguientes políticas :

Impresión	
En la nueva página de gestión de impresoras se centraliza la gestión de todas las impresoras CUPS nativas.	
Impresión Aplicado de forma local	Habilitar la impresión
Vista previa de impresión Se ha heredado de Google de f...	Permitir vista previa de impresión Permitir utilizar la vista previa de impresión
Envío a Google Cloud Print Se ha heredado de Google de f...	Permitir el envío de documentos a Google Cloud Print
Proxy de Google Cloud Print Se ha heredado de Google de f...	Permitir utilizar Chrome como proxy para Google Cloud Print
Vista previa de impresión predeterminada Se ha heredado de Google de f...	Selección de impresora predeterminada Utilizar comportamiento de impresión predeterminado
Gestión de impresoras nativas Aplicado de forma local	Añadir nuevas impresoras CUPS en el dispositivo Permitir que los usuarios añadan impresoras
Modo de impresión en color predeterminado Se ha heredado de Google de f...	Color



UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
SECRETARÍA DE DESARROLLO INSTITUCIONAL
Manual de enrolamiento MDM y puesta a punto de dispositivos v.1.4

Restringir el modo de impresión en color Se ha heredado de Google de f... 	No restringir el modo de impresión en color ▼
Configuración de caras predeterminada Se ha heredado de Google de f... 	A una cara ▼
Restringir caras Se ha heredado de Google de f... 	No restringir el modo de impresión a doble cara ▼
Información del trabajo de impresión nativo Se ha heredado de Google de f... 	Compartir la cuenta de usuario y el nombre de archivo en el trabajo de impresión No incluir la cuenta de usuario ni el nombre de archivo en el trabajo de impresión ▼
Restringir el modo de impresión con PIN Se ha heredado de Google de f... 	No restringir el modo de impresión con PIN ▼
Modo predeterminado de impresión con PIN Se ha heredado de Google de f... 	Con PIN ▼

Imagen 96: Impresión

En la sección de **Experiencia de usuario** se deberán aplicar las siguientes políticas :

Experiencia de usuario

Marcadores gestionados
Se ha heredado de Google de f...

Nombre de la carpeta de marcadores gestionados

Gestionar marcadores del usuario

No se ha configurado ningún marcador en esta unidad organizativa. +

Barra de marcadores
Se ha heredado de Google de f...

Permitir que el usuario decida ▼

Posición de la estantería
Se ha heredado de Google de f...

Permitir que el usuario decida ▼

Edición de marcadores
Aplicado de forma local ▼

Inhabilitar edición de marcadores ▼

Ubicación de las descargas
Se ha heredado de Google de f...

Establecer la carpeta Descargas local como ubicación predeterminada, pero permitir que el usuario la cambie

Imagen 97: Experiencia de usuario



Servicio de revisión ortográfica Aplicado de forma local ▾ 	Habilitar el servicio web de revisión ortográfica ▾	
Traductor de Google Se ha heredado de Google de f... 	Permitir que el usuario decida ▾	
Páginas de error alternativas Se ha heredado de Google de f... 	Permitir que el usuario decida ▾	
Herramientas de desarrollo Aplicado de forma local ▾ 	No permitir nunca el uso de herramientas de desarrollo integradas ▾	
Autocompletar formulario Aplicado de forma local ▾ 	No autocompletar nunca los formularios ▾	
Precarga de DNS Aplicado de forma local ▾ 	No obtener nunca DNS previamente ▾ Este ajuste permite controlar la obtención previa de DNS, la conexión previa de TCP y SSL, y la carga previa de páginas web.	
Predicción de red Se ha heredado de Google de f... 	Permitir que el usuario decida ▾	
Acceso mediante inicio de sesión múltiple Se ha heredado de Google de f... 	<p>Acceso mediante inicio de sesión múltiple</p> <p>El usuario gestionado debe ser el usuario principal (se permiten usuarios secundarios) ▾</p> <p>Los usuarios no tendrán habilitado el inicio de sesión múltiple cuando se apliquen certificados de inspección de SSL. 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.</p>	
Iniciar sesión en cuentas secundarias Se ha heredado de Google de f... 	Permitir que los usuarios inicien sesión en cualquier cuenta de Google secundaria ▾	
Escritorio unificado (BETA) Se ha heredado de Google de f... 	<p>Hacer que el modo de escritorio unificado no esté disponible para el usuario ▾</p> <p>En el modo de escritorio unificado, las aplicaciones pueden ocupar varias pantallas.</p>	
Recopilación de registros de eventos de WebRTC Se ha heredado de Google de f... 	<p>Recopilación de registros de eventos de WebRTC</p> <p>Permitir que se recojan registros de eventos WebRTC ▾</p> <p>Este ajuste permite que los servicios de Google llamen a la API de Chrome para recopilar los eventos de WebRTC de los clientes que han dado su consentimiento. El valor inicial se hereda de la configuración de subida de registros de Hangouts Meet.</p>	

Imagen 98: Experiencia de usuario

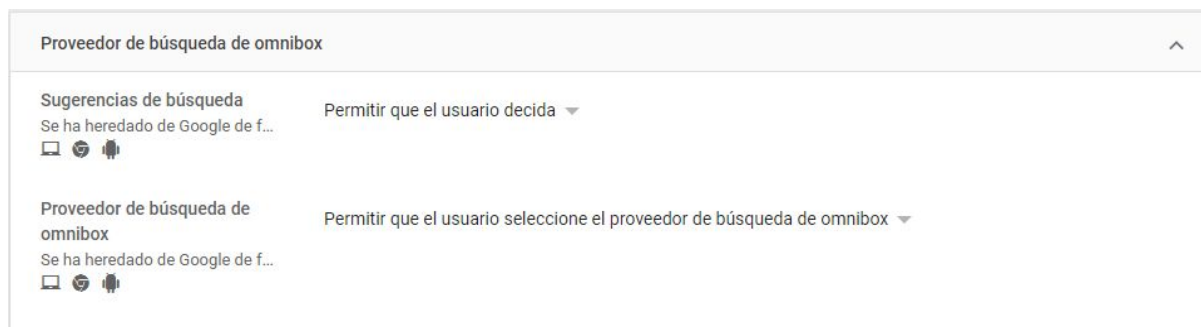


Imagen 99: Proveedor de búsqueda de omnibox

En la sección de **Hardware** se deberán aplicar las siguientes políticas :

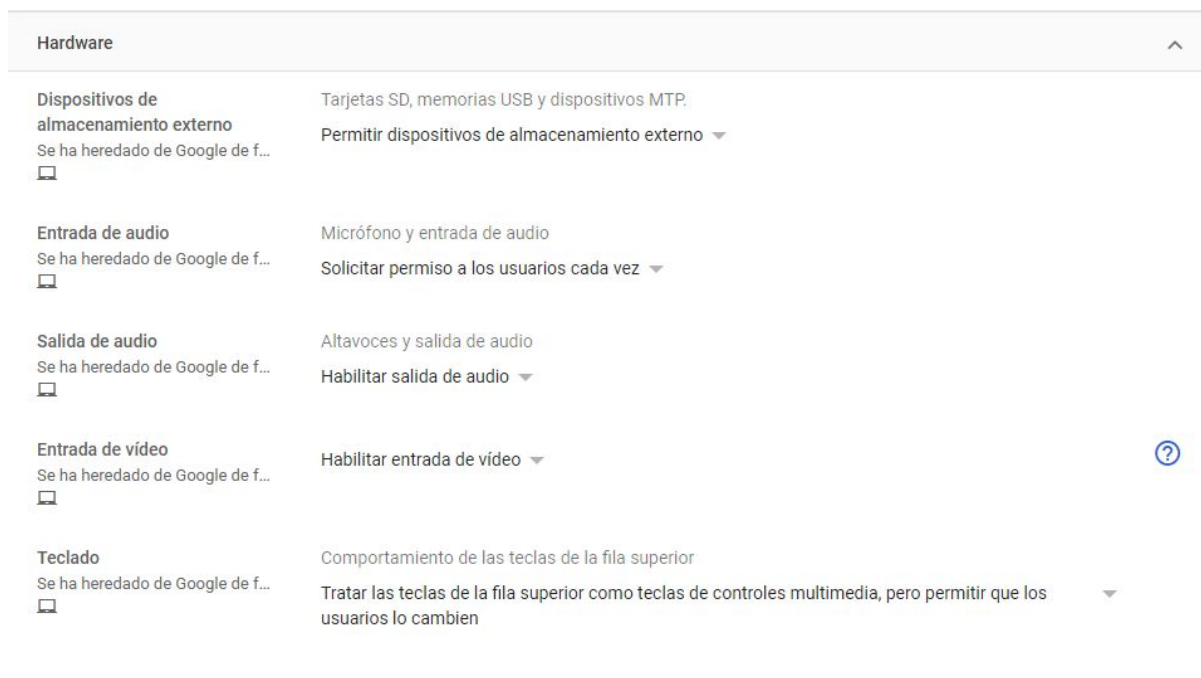


Imagen 100: Hardware



En la sección de **Verificación de usuarios** se deberán aplicar las siguientes políticas :

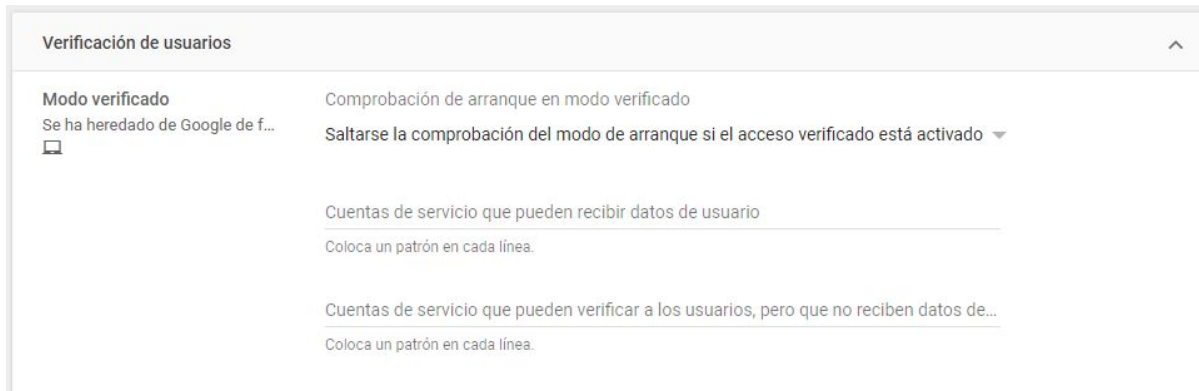


Imagen 101: Verificación de usuarios

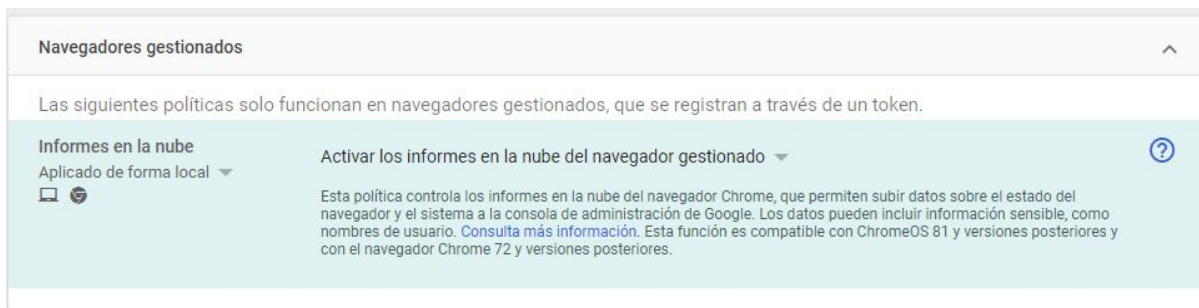


Imagen 102: Navegadores gestionados



En la sección de **Navegación Segura de Chrome** se deberán aplicar las siguientes políticas :

Navegación Segura

Aplicado de forma local

Ayudar a mejorar la función Navegación Segura

Se ha heredado de Google de f...

Dominios incluidos en la lista blanca de Navegación Segura

Se ha heredado de Google de f...

Restricciones de descarga

Aplicado de forma local

Inhabilitar la omisión de las advertencias de Navegación Segura

Aplicado de forma local

Habilitar siempre la función Navegación Segura

Permitir que el usuario decida

Dominios incluidos en lista blanca

Bloquear descargas potencialmente peligrosas

No permitir que el usuario omita las advertencias de Navegación Segura

Establecer advertencia de protección de contraseña

Activar al reutilizar una contraseña en una página de phishing

URL para cambiar la contraseña

URLs de acceso

Introduce la lista de los dominios que quieres que se excluyan de las comprobaciones de Navegación Segura. Indica cada elemento en una línea.

Introduce la URL de la página web en la que los usuarios pueden cambiar su contraseña.

Introduce la lista de las URL de acceso de empresa en las que el servicio de protección de contraseña debe capturar la huella digital de la contraseña. Indica cada elemento en una línea.

Más información

Más información

Más información

?

Imagen 103: Navegación segura de chrome



En la sección de Compatibilidad de navegadores antiguos asignar las siguientes políticas

Compatibilidad con navegadores antiguos	
Compatibilidad con navegadores antiguos Se ha heredado de Google de f...	Inhabilitar compatibilidad con navegadores antiguos
Retraso antes de cambiar de navegador Se ha heredado de Google de f...	Retraso (s) Si el valor seleccionado es mayor que 0, Chrome mostrará un mensaje indicando cuántos segundos transcurrirán antes de cambiar de navegador.
Usar lista de sitios de Internet Explorer Se ha heredado de Google de f...	No usar la política SiteList de Internet Explorer como fuente de reglas
Lista de sitios web para gestionar la compatibilidad con navegadores antiguos Se ha heredado de Google de f...	URL del archivo XML de la lista de sitios web
URL de la lista de sitios web que se abren en los dos navegadores Se ha heredado de Google de f...	URL del archivo XML de la lista de sitios web
Sitios web que se abren en el navegador alternativo Se ha heredado de Google de f...	URLs de los sitios web que se abren en el navegador alternativo
Sitios web que se abren en los dos navegadores Se ha heredado de Google de f...	URLs de los sitios web que se abren en los dos navegadores
Parámetros del navegador alternativo Se ha heredado de Google de f...	Parámetros de la línea de comandos Uno por línea. Parámetros del navegador alternativo. Si un parámetro contiene \$(url), se sustituye por la URL. Si no, la URL se añade al final de la línea de comandos.
Ruta del navegador alternativo Se ha heredado de Google de f...	Ruta del navegador alternativo Si no se configura esta política, se utilizará una predeterminada específica de la plataforma.
Parámetros de Chrome Se ha heredado de Google de f...	Parámetros de la línea de comandos Solo en Windows; uno por línea. Parámetros para iniciar Chrome desde el navegador alternativo. Si un parámetro contiene \$(url), se sustituye por la URL. Si no, la URL se añade al final de la línea de comandos.
Ruta de Chrome Se ha heredado de Google de f...	Ruta del ejecutable de Chrome Solo en Windows. Ruta del ejecutable que se iniciará al cambiar del navegador alternativo a Chrome. Si no se configura, el navegador alternativo detectará la ruta de Chrome automáticamente.
Mantener la última pestaña de Chrome Se ha heredado de Google de f...	Mantener al menos una pestaña de Chrome abierta Esta política permite controlar si Chrome se debe cerrar por completo o no cuando la última pestaña vaya a cambiar al navegador alternativo.

Imagen 104: Compatibilidad con navegadores antiguos

En la sección de otros ajustes

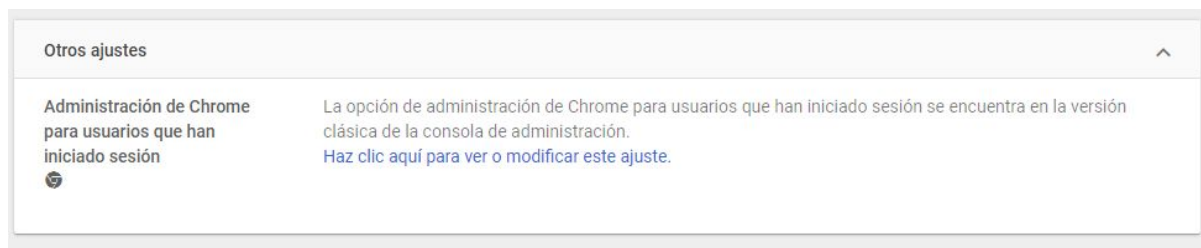


Imagen 105: Otros ajustes

Configuración de dispositivo

La configuración del dispositivo administra directamente a las chromebooks para establecer políticas que restrinjan la forma en la que serán empleados estos dispositivos.

En la interfaz de Google Admin ir al apartado de **Dispositivos**

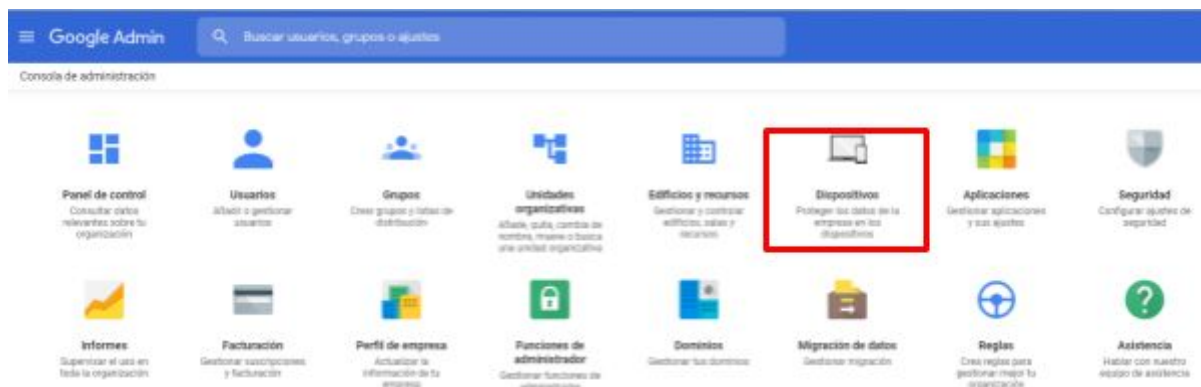


Imagen 106: Elegir Dispositivos



En el menú lateral escoger **Administración de Chrome**

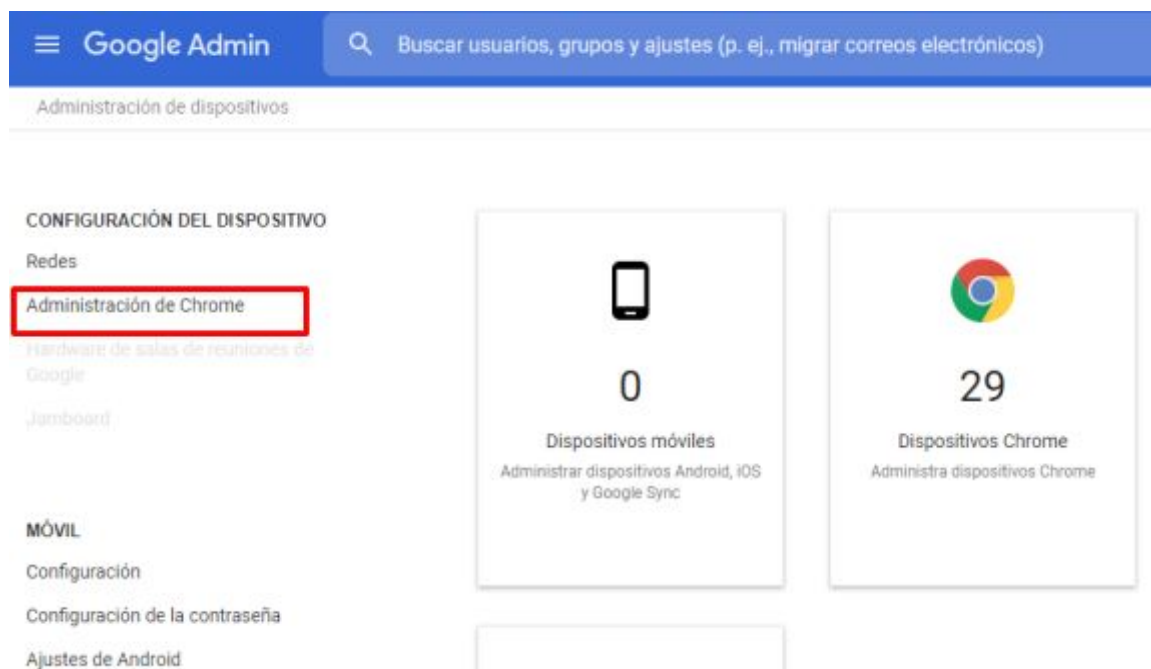


Imagen 107: Elegir Administración de Chrome

En el menú que se despliega de Administración de Chrome se deberá escoger **Configuración del Dispositivo**

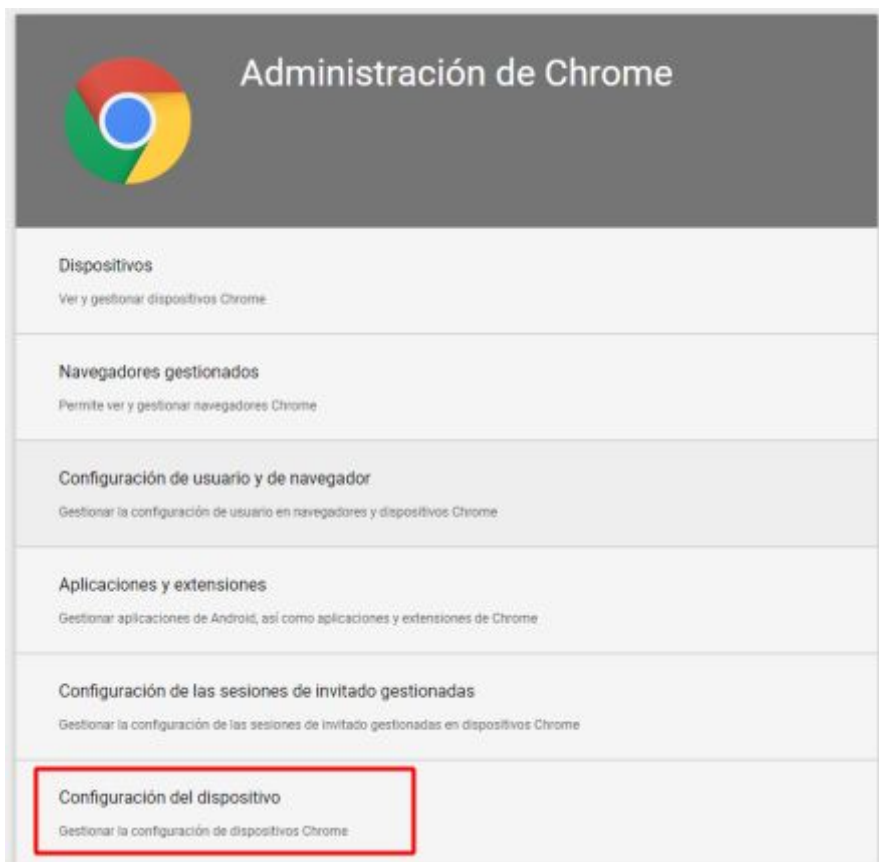


Imagen 108: Ingresar a la Configuración del dispositivo



Verifique que se encuentra en la sección de **Configuración del Dispositivo**



Imagen 109: Verificar sección de configuración del dispositivo

Se debe elegir la **UNIDAD ORGANIZATIVA** a la que queremos aplicar los cambios, para fines de muestra se asignan en este manual los cambios a la **UNIDAD ORGANIZATIVA Pruebas**

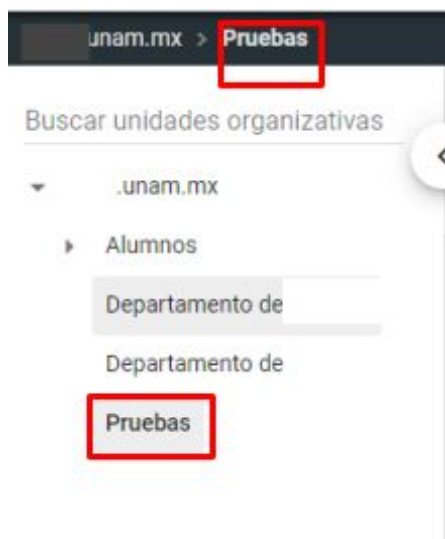


Imagen 110: Asignar a la unidad organizativa



Añadir las opciones de **Registro y acceso** que se muestran a continuación:

Registro y acceso

Obligación de volver a realizar el registro
Aplicado de forma local

Forzar que se vuelvan a registrar automáticamente los dispositivos en este dominio después de que se borren sus datos

Acceso verificado
Se ha heredado de cele.unam....

Habilitar la protección de contenido

Modo verificado
Se ha heredado de Google de f...

Requerir arranque en modo verificado para permitir el acceso verificado

Instrucciones de devolución de dispositivo inhabilitado
Aplicado de forma local

Servicios con acceso completo

Cuentas de servicio que pueden recibir el ID de dispositivo. Coloca un patrón en cada línea.

Servicios con acceso limitado

Cuentas de servicio que pueden verificar los dispositivos, pero que no reciben el ID de dispositivo. Coloca un patrón en cada línea.

Instrucciones de devolución de dispositivo inhabilitado

Favor de devolver el dispositivo.
Gracias

Texto personalizado que se mostrará debajo del mensaje de dispositivo bloqueado. Te recomendamos que incluyas una dirección de devolución y un número de teléfono de contacto en tu mensaje.

Segundo factor integrado de FIDO
Aplicado de forma local

Habilitar el segundo factor integrado de Titan M en los dispositivos compatibles con FIDO

Inhabilitar el segundo factor integrado

Imagen 111: Registro y acceso



Para la sección de Configuración de **Inicio de Sesión** establecer la siguiente configuración y agregar en imagen de fondo de pantalla del dispositivo el fondo de pantalla que se muestra detrás de la pantalla de inicio de sesión :

Configuración de inicio de sesión

Modo invitados

Aplicado de forma local

Inhabilitar el modo invitados

Restricción de inicio de sesión

Se ha heredado de Google de f...

Permitir que cualquier usuario inicie sesión

Autocompletar dominio

Aplicado de forma local

Usar el nombre de dominio que aparece abajo para autocompletar el dominio al iniciar sesión

Autocompletar el prefijo del dominio

nombredeusuario@entidadunam.mx

Pantalla de inicio de sesión

Aplicado de forma local

Mostrar nombres de usuario y fotos en la pantalla de inicio de sesión

No mostrar nunca nombres de usuario ni fotos

Horario con menos restricciones

La configuración del horario con menos restricciones se encuentra en la versión clásica de la consola de administración.

Haz clic aquí para ver o modificar este ajuste.

Imagen de fondo de pantalla del dispositivo

Aplicado de forma local

Subir

Ver

Eliminar

Configura la imagen del fondo de pantalla del dispositivo que se mostrará en la pantalla de inicio de sesión cuando ningún usuario haya iniciado sesión aún en él. La imagen debe estar en formato JPEG y su tamaño no debe superar los 16 MB.

Imagen 112: Configuración de inicio de sesión

73



UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
SECRETARÍA DE DESARROLLO INSTITUCIONAL
Manual de enrolamiento MDM y puesta a punto de dispositivos v.1.4

Datos de usuario
Aplicado de forma local ▼

Borrar toda la información del usuario local, la configuración y el estado después de cada cierre de sesión
Borrar todos los datos de usuario locales ▼

Redireccionamiento del proveedor de identidades de inicio de sesión único
Se ha heredado de Google de f...

Redirigir a los usuarios al proveedor de identidades para el inicio de sesión único (SSO) basado en SAML
Dirigir a los usuarios a la pantalla de inicio de sesión de Google predeterminada ▼



Comportamiento de cookies de inicio de sesión único
Se ha heredado de Google de f...

Inhabilitar la transferencia de cookies de inicio de sesión único basado en SAML a la sesión de usuario durante el acceso
Advertencia: Esta política solo es pertinente si se ha configurado el SSO basado en SAML en los dispositivos Chrome.
[Más información](#)

Permisos de la cámara con inicio de sesión único
Se ha heredado de Google de f...

Lista blanca de permisos de la cámara con inicio de sesión único
Advertencia: Al habilitar esta política, permites que terceros accedan a las cámaras de tus usuarios en su nombre. Para obtener más información sobre el inicio de sesión único y los permisos de la cámara, consulta el Centro de Ayuda.



Certificados de cliente de inicio de sesión único
Se ha heredado de Google de f...

Seleccionar automáticamente el certificado de cliente de estos sitios web de inicio d...
Consulta la [documentación sobre políticas de Chromium para ver el formato de este ajuste](#).

Control de accesibilidad
Aplicado de forma local ▼

Desactivar la configuración de accesibilidad en la pantalla de inicio de sesión al cerrar sesión ▼

Idioma de inicio de sesión

La configuración del idioma de inicio de sesión se encuentra en la versión clásica de la consola de administración.
[Haz clic aquí para ver o modificar este ajuste.](#)

Teclado de inicio de sesión
Aplicado de forma local ▼

Crear una lista ordenada de los teclados que se pueden usar en la pantalla de inicio de sesión

🔍 Filtrar por diseño de teclado	Ordenar teclados
<input type="checkbox"/> Teclado alemán	Teclado latinoamericano ✕
<input type="checkbox"/> Teclado alemán Neo 2	
<input type="checkbox"/> Teclado ampliado de EE. UU.	
<input type="checkbox"/> Teclado belga [Alemán (Alemania) - Deutsche]	
<input type="checkbox"/> Teclado belga [Francés (Francia) - Français]	
<input type="checkbox"/> Teclado belga [Neerlandés - Nederlands]	
<input type="checkbox"/> Teclado brasileño	
<input type="checkbox"/> Teclado catalán	



Para la sección de **Configuración de actualización de dispositivos** establecer la siguiente configuración:

Configuración de actualización de dispositivos

Configuración de actualizaciones automáticas

Aplicado de forma local

Actualizaciones automáticas

Permitir actualizaciones automáticas

Definir la versión máxima de Google Chrome

79.*

Los dispositivos de esta unidad organizativa se actualizarán de acuerdo con las actualizaciones controladas por la aplicación definidas más abajo. Esta política no tendrá ningún efecto mientras las actualizaciones controladas por la aplicación estén configuradas.

Plan de implementación

Implementar actualizaciones según una programación específica

Calendario de staging

Transcurridos 15 días, actualizar un 25 % de los dispositivos.

Transcurridos 25 días, actualizar un 50 % de los dispositivos.

Transcurridos 28 días, actualizar el 100 % de los dispositivos.

Reiniciar automáticamente al completar actualizaciones

Permitir reinicios automáticos

Actualizaciones por datos móviles

Permitir las actualizaciones automáticas solo por Wi-Fi y Ethernet

Actualizaciones controladas por la aplicación

Se ha heredado de Google de f...

Permitir que la aplicación controle la versión del sistema operativo

No se ha configurado ninguna aplicación.

SELECCIONAR UNA APLICACIÓN

Actualizaciones controladas por kiosco

Se ha heredado de Google de f...

Permitir que la aplicación de kiosco controle la versión del SO

No permitir que la aplicación de kiosco controle la versión del SO

Advertencia: Esta política está inhabilitada y no se puede configurar porque las actualizaciones automáticas están activadas. Más información

Versión

Se ha heredado de Google de f...

Canal estable

El canal de versiones no se puede cambiar en el nivel organizativo superior.

Imagen 113: Configuración de inicio de sesión



Para la configuración de la sección de **Configuración de kiosko** establecer la siguiente configuración:

Configuración de kiosko

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

- Configurar aplicaciones de kiosco
- Configurar una aplicación para que se inicie automáticamente
- Configurar otros ajustes de la aplicación con inicio automático, por ejemplo:
 - Supervisión del estado del dispositivo
 - Subida de registros del sistema del dispositivo
 - Rotación de pantalla

Sesión de invitado gestionada
Se ha heredado de Google de f...

No permitir sesiones de invitado gestionadas ▼

Antes de habilitar esta función, asigna un nombre visible a la sesión en la página de configuración de la sesión de invitado gestionada.

Envío de alertas sobre el estado del dispositivo de kiosco
Aplicado de forma local ▼

☐ Recibir alertas por correo electrónico ☒ Recibir alertas por SMS

Información de contacto para alertas sobre el estado del dispositivo de kiosco
Se ha heredado de Google de f...

Correos electrónicos para recibir alertas
Direcciones de correo electrónico (p. ej., usuario@example.com); una por línea

Teléfonos móviles para recibir alertas
Números de teléfono (p. ej., +34XXXXXXZZZ, +34AAABBBCCC); uno por línea

Imagen 114: Configuración de kiosko

Para la sección **Informes de usuarios y de dispositivos** establecer la siguiente configuración:

Informes de usuarios y de dispositivos

Informes de dispositivo
Se ha heredado de Google de f...

Habilitar los informes de estado del dispositivo ▼

Habilitar el seguimiento de los usuarios de dispositivos recientes ▼

Notificaciones de dispositivos inactivos
Aplicado de forma local ▼

Informes de notificación de dispositivos inactivos

Inhabilitar notificaciones de dispositivos inactivos ▼

Intervalo de inactividad (días)
3
Los dispositivos que se hayan sincronizado por última vez antes de este intervalo se consideran inactivos.

Frecuencia de notificación (días)
7
Recibir un informe de dispositivos inactivos con esta frecuencia.

Direcciones de correo electrónico para recibir informes de notificación
responsable@entidad.unam.mx

Introduce una lista de las direcciones de correo electrónico a las que enviar informes de dispositivos inactivos (una dirección por línea).

Informes anónimos sobre métricas
Aplicado de forma local ▼

No enviar métricas a Google nunca ▼

Imagen 115: Informes de usuarios y de dispositivos



En la sección de **Batería y apagado** establecer las siguientes políticas:

Batería y apagado	
Gestión de energía Aplicado de forma local ▼	Gestión de la batería en la pantalla de inicio de sesión No permitir que el dispositivo entre en modo de suspensión o se apague cuando esté inactivo en la pantalla de inicio de sesión
Reinicio programado Se ha heredado de Google de f...	Límite de tiempo de funcionamiento Días que quedan para reiniciar; deja el campo en blanco si no quieres configurar esta opción
Permitir el apagado Aplicado de forma local ▼	Solo permitir a los usuarios apagar el dispositivo con el botón de encendido físico ▼

Imagen 116: Batería y apagado

En la sección de **Otros ajustes** establecer las siguientes políticas:

Otros ajustes	
Google Cloud Print	La configuración de Google Cloud Print se encuentra en la versión clásica de la consola de administración. Haz clic aquí para ver o modificar este ajuste.
Plantilla de nombre de host de red de dispositivo Se ha heredado de Google de f...	Plantilla de nombre de host de red de dispositivo Selecciona el nombre de host que pasa al servidor DHCP con la solicitud de DHCP. Posibles formatos: \${ASSET_ID}, \${SERIAL_NUM} y \${MAC_ADDR}.
Zona horaria Aplicado de forma local ▼	Zona horaria del sistema America/Mexico_City - hora central GMT-06:00 ▼ Detección automática de la zona horaria del sistema Enviar todos los datos de ubicación ▼
Itinerancia de datos móviles Se ha heredado de Google de f...	No permitir la itinerancia de datos de móviles ▼
Lista blanca de dispositivos USB extraíbles Se ha heredado de Google de f...	Lista blanca de dispositivos USB extraíbles Para identificar un hardware específico, introduce pares hexadecimales de identificador de proveedor de USB e identificador de producto separados por dos puntos. Coloca cada uno de estos pares en líneas diferentes.
Bluetooth Se ha heredado de Google de f...	Inhabilitar Bluetooth en el dispositivo No inhabilitar Bluetooth ▼

<p>Limitar el ancho de banda del dispositivo</p> <p>Aplicado de forma local ▼</p>	<p>Limitar el consumo del ancho de banda de red en los dispositivos</p> <p>Inhabilitar la limitación de red ▼</p>	?
<p>Actualización del firmware de TPM</p> <p>Se ha heredado de Google de f...</p>	<p>Impedir que los usuarios actualicen el firmware de TPM ▼</p> <p>Con este ajuste puedes impedir o permitir que los usuarios actualicen el firmware de TPM. Ten en cuenta que, al actualizarlo, se puede restablecer la configuración de fábrica del dispositivo y, si fallan varias actualizaciones, el dispositivo puede dejar de funcionar. Antes de modificar esta política, consulta esta información sobre el proceso de actualización.</p>	
<p>Máquinas virtuales</p> <p>Se ha heredado de Google de f...</p>	<p>Bloquear el uso de las máquinas virtuales necesarias para el funcionamiento de las aplicaciones de Linux ▼</p>	

Imagen 117: Otros ajustes

Gestión de aplicaciones a instalar

Para instalar las aplicaciones deseada y que estas se propaguen se debe acceder desde la consola de administración de google a **Dispositivos**

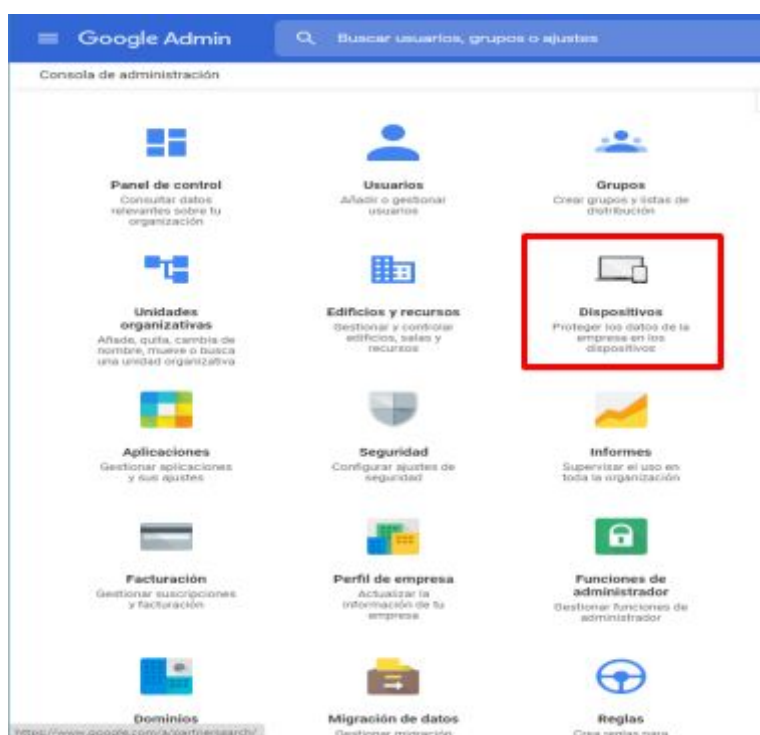


Imagen 118: Seleccionar Dispositivos



Acceder a la sección de **Administración de Chrome** en la parte superior izquierda

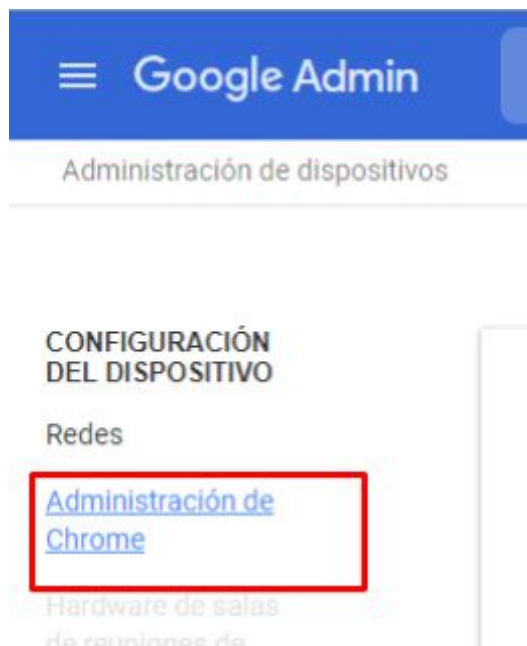


Imagen 119: accede a Administración de Chrome

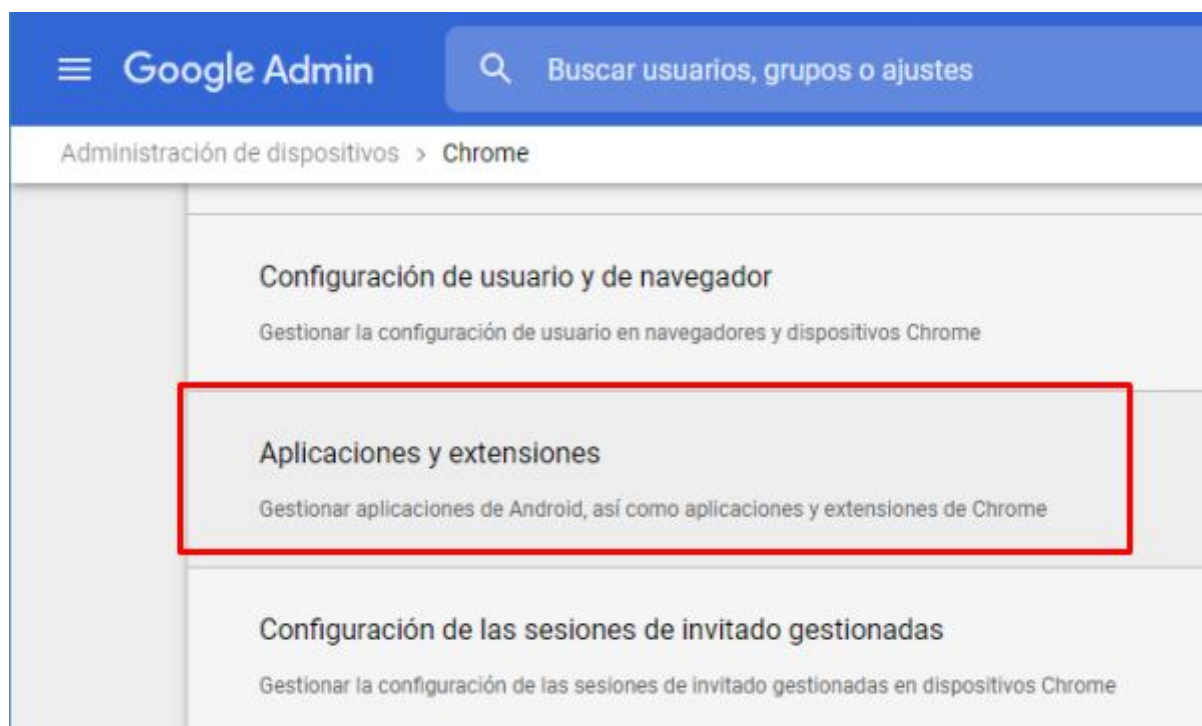


Imagen 120: acceder a Aplicaciones y extensiones

Fijar la unidad organizativa a la cual se desea agregar las aplicaciones

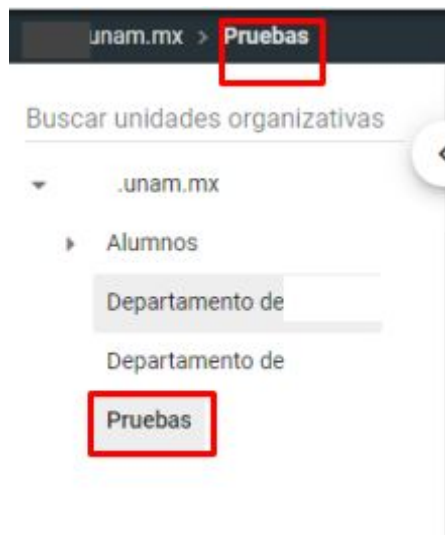


Imagen 121: Fijar unidad organizativa

Agregar las aplicaciones deseadas dando clic en el signo + del extremos inferior derecho donde se pueden instalar aplicaciones de Chrome Webstore, Playstore y más.

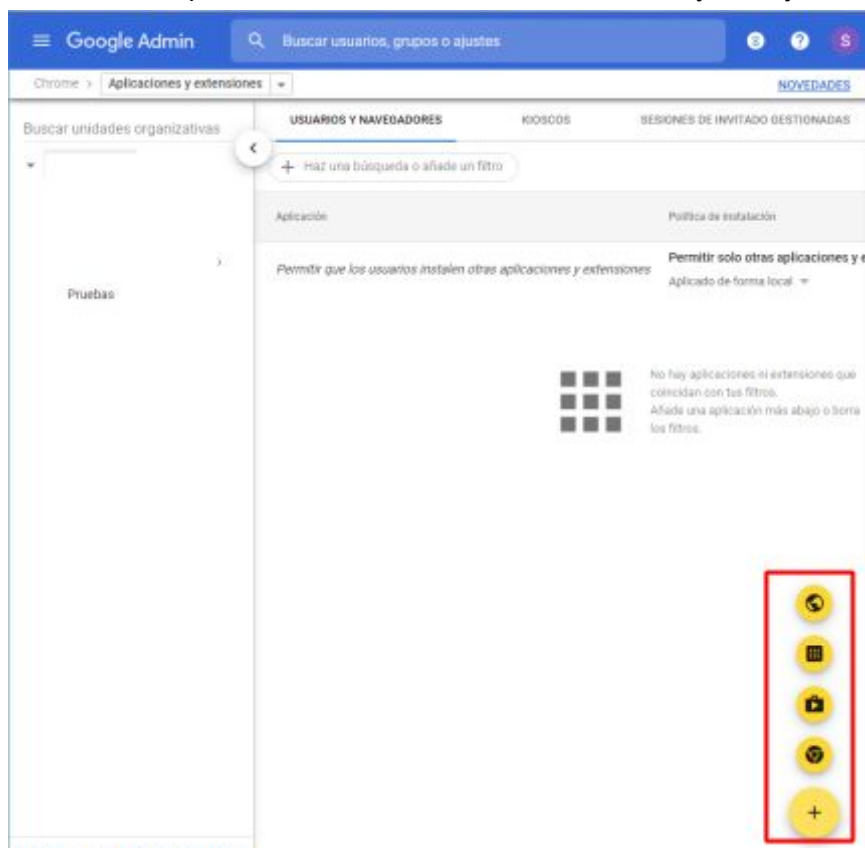


Imagen 122: Añadir aplicaciones



Al elegir añadir una aplicación desde la Play Store, por ejemplo, se pueden instalar aplicaciones que normalmente se añaden en un móvil con Android, se busca la aplicación a instalar desde el recuadro de búsqueda

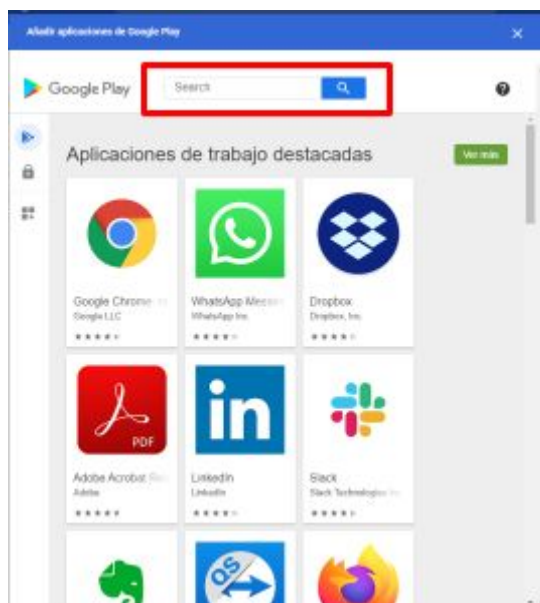


Imagen 123: Buscar la aplicación

Después de buscar la aplicación a instalar se da clic en la misma

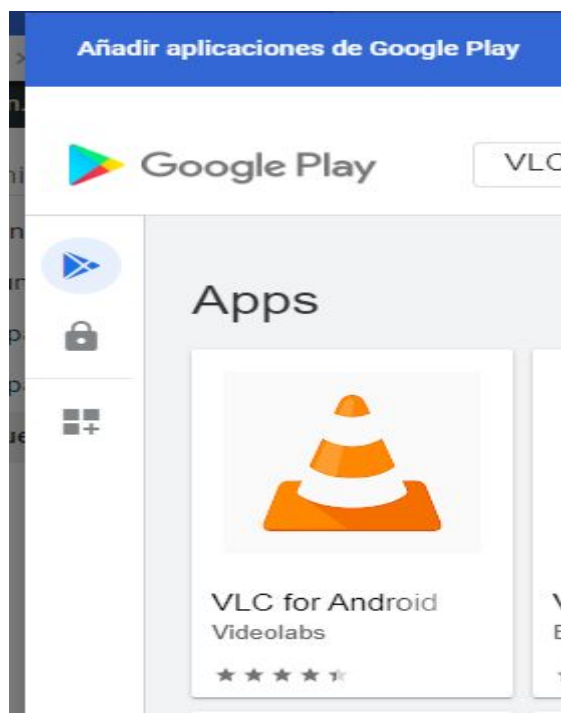


Imagen 124: Elegir la aplicación a instalar



Se añade la aplicación dando clic en el recuadro de **Seleccionar**

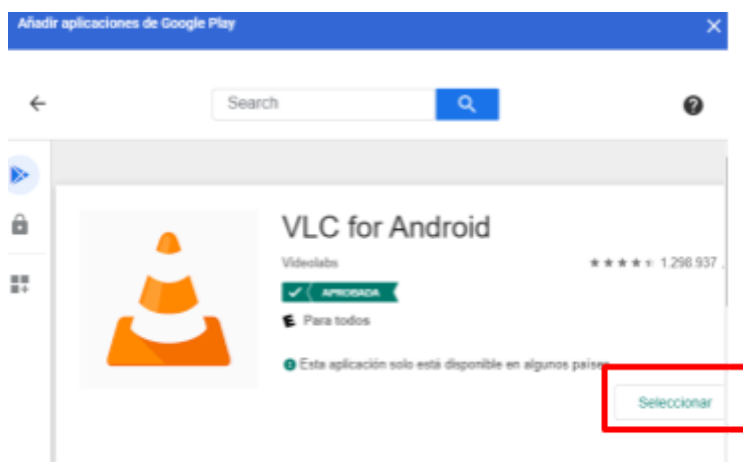


Imagen 125: Dar clic en Seleccionar

No olvidar guardar los cambios de las aplicaciones que se vayan añadiendo

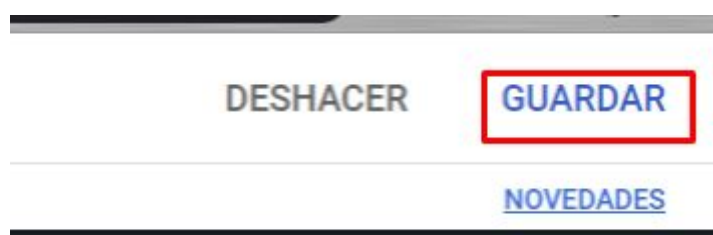


Imagen 126: Guardar cambios

Se recomienda el siguiente paquete base de aplicaciones, la entidad deberá añadir las aplicaciones que con convenientes











USUARIOS Y NAVEGADORES		
+ Haz una búsqueda o añade un filtro		
Aplicación	Política de instalación	
 Adobe Acrobat Reader com.adobe.reader	Forzar la instalación	①
	Se ha añadido de forma local	
 Evernote com.evernote	Forzar la instalación y fijar	①
	Se ha añadido de forma local	
 Google Classroom mfhehppjhmnmifbopchdfidgimhfntk	Forzar la instalación y fijar	
	Se ha añadido de forma local	
 VLC for Android org.videolan.vlc	Forzar la instalación	①
	Se ha añadido de forma local	
 Google Drive com.google.android.apps.docs	Forzar la instalación y fijar	①
	Se ha añadido de forma local	
 Messenger com.facebook.orca	Forzar la instalación	①
	Se ha añadido de forma local	
 PDF: Merge & Download & View dooiadpbpkhbjlmcfcfcmoeqkphbjbde	Permitir la instalación	
	Se ha añadido de forma local	
 Dropbox ioekoebjcdmniefjknokhahfcljcdl	Forzar la instalación	
	Se ha añadido de forma local	
 Kahoot! no.mobitroll.kahoot.android	Forzar la instalación	①
	Se ha añadido de forma local	
 Office ndjpnldacallmjembaebfdecfnkepb	Forzar la instalación	
	Se ha añadido de forma local	

Imagen 127:Aplicaciones instaladas en la consola de google

Deberá activar las aplicaciones android dando click en el signo de admiración que se encuentra enseguida de la aplicación android y permitiendo la instalación de aplicaciones



Imagen 128: Permitir aplicaciones android



Por último deberá aceptar los términos para habilitar aplicaciones de Android en toda tu organización.

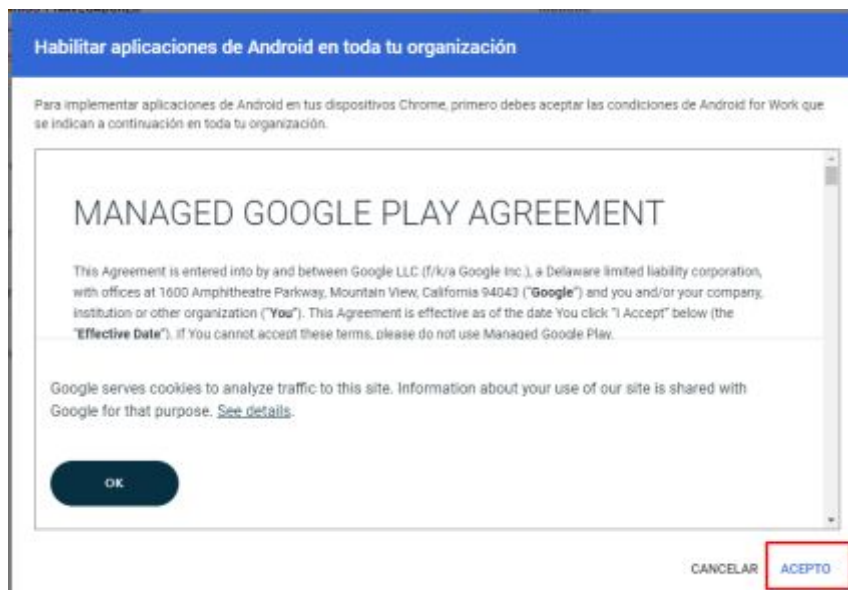


Imagen 129: Habilitar aplicaciones android

Asignación de Dispositivos a unidades organizativas

Se deberá mover los dispositivos deseados a la unidad organizativa que se necesite para aplicar sobre éste las políticas asociadas a dicha unidad organizativa

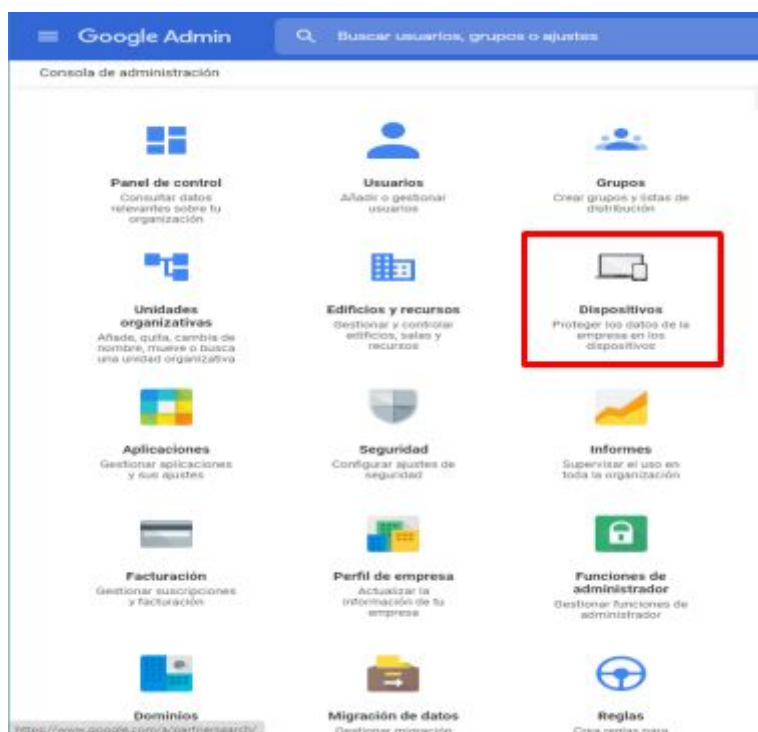


Imagen 130: Ingresar a sección de dispositivos

Seleccionar dispositivos Chrome

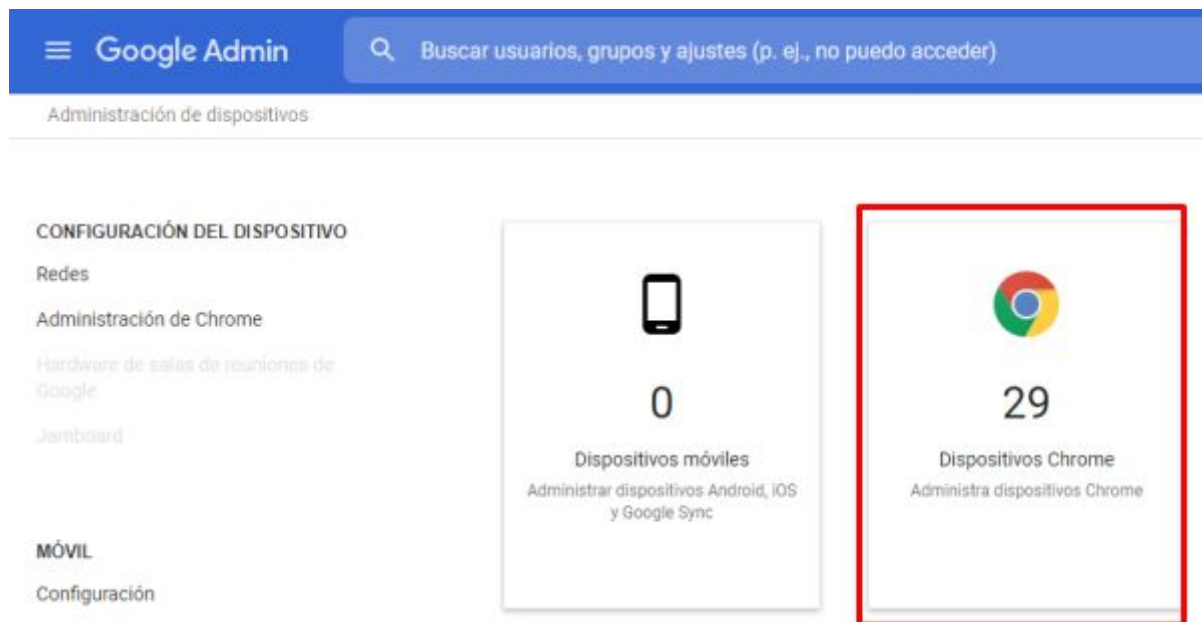


Imagen 131: Seleccionar Dispositivos Chrome

Se deberán elegir los dispositivos que se desean asignar a determinada unidad organizativa dependiendo de sus políticas asignadas

Seleccionados: 3 de 29 ✕			
Estado: Aprovisionado		+ Haz una búsqueda o	
<input type="checkbox"/>	Número de serie	Estado	ID de recurso
<input checked="" type="checkbox"/>	5CD9242LZH	Aprovisionado	
<input checked="" type="checkbox"/>	5CD9242L75	Aprovisionado	
<input type="checkbox"/>	5CD9242M0Z	Aprovisionado	
<input type="checkbox"/>	5CD9242LTT	Aprovisionado	
<input checked="" type="checkbox"/>	5CD9242L5P	Aprovisionado	
<input type="checkbox"/>	5CD9242LWS	Aprovisionado	
<input type="checkbox"/>	5CD9242KZ4	Aprovisionado	

Imagen 132: Seleccionar dispositivos a asignar a unidad organizativa

En la esquina superior derecha de la consola de google aparecen 3 opciones para realizar sobre estos dispositivos, una de estas opciones es mover el dispositivo seleccionado a una unidad organizativa en específico, dar clic en **Mover dispositivos seleccionados**

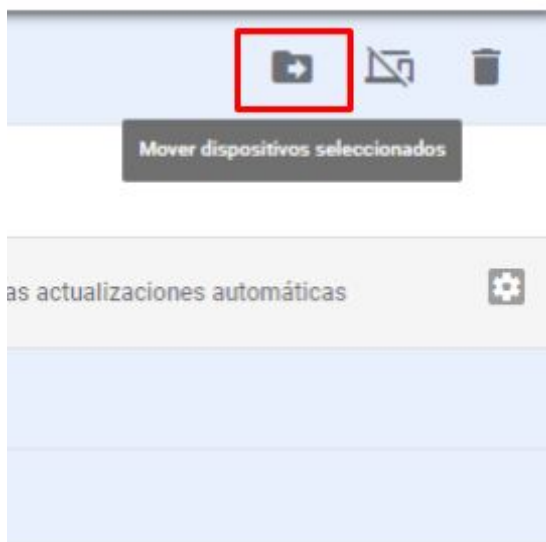


Imagen 133: Mover dispositivos seleccionados

Elegir la unidad organizativa destino de los dispositivos seleccionados y dar clic en **Mover**

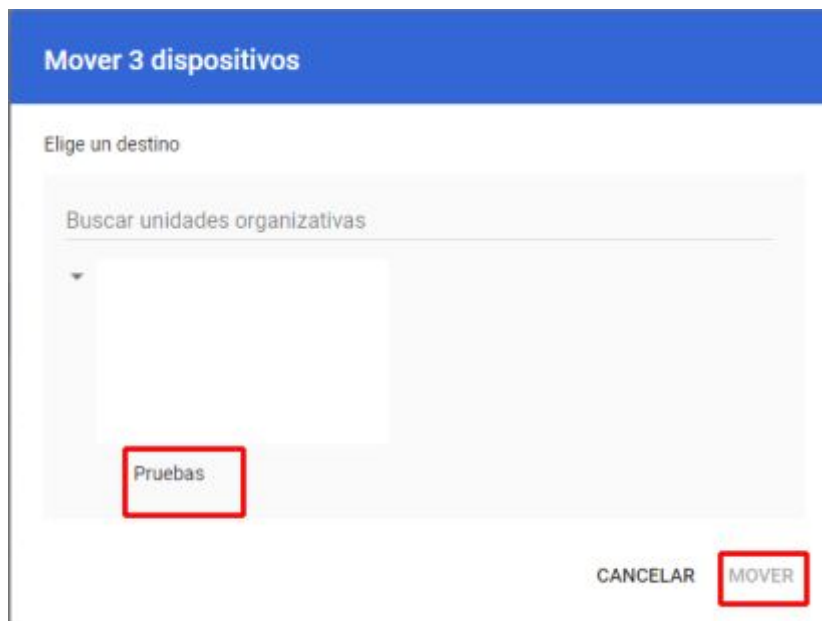


Imagen 134: Elegir unidad organizativa



Powerwash

En caso de que exista la necesidad de restablecer la chromebook y borrar sus datos se puede realizar :

Ctrl + Alt + Mayús + R

Y en el cuadro que aparece dar clic en **Powerwash**