



**Carga de extensión IMTLazarus en Google
Workspace y medidas de seguridad**
Administradores IMTLazarus

C Arteagabeitia 41, Barakaldo
48902, Vizcaya, Basque Country (Spain)

(+34) 94 437 78 01



www.imtlazarus.com

Índice

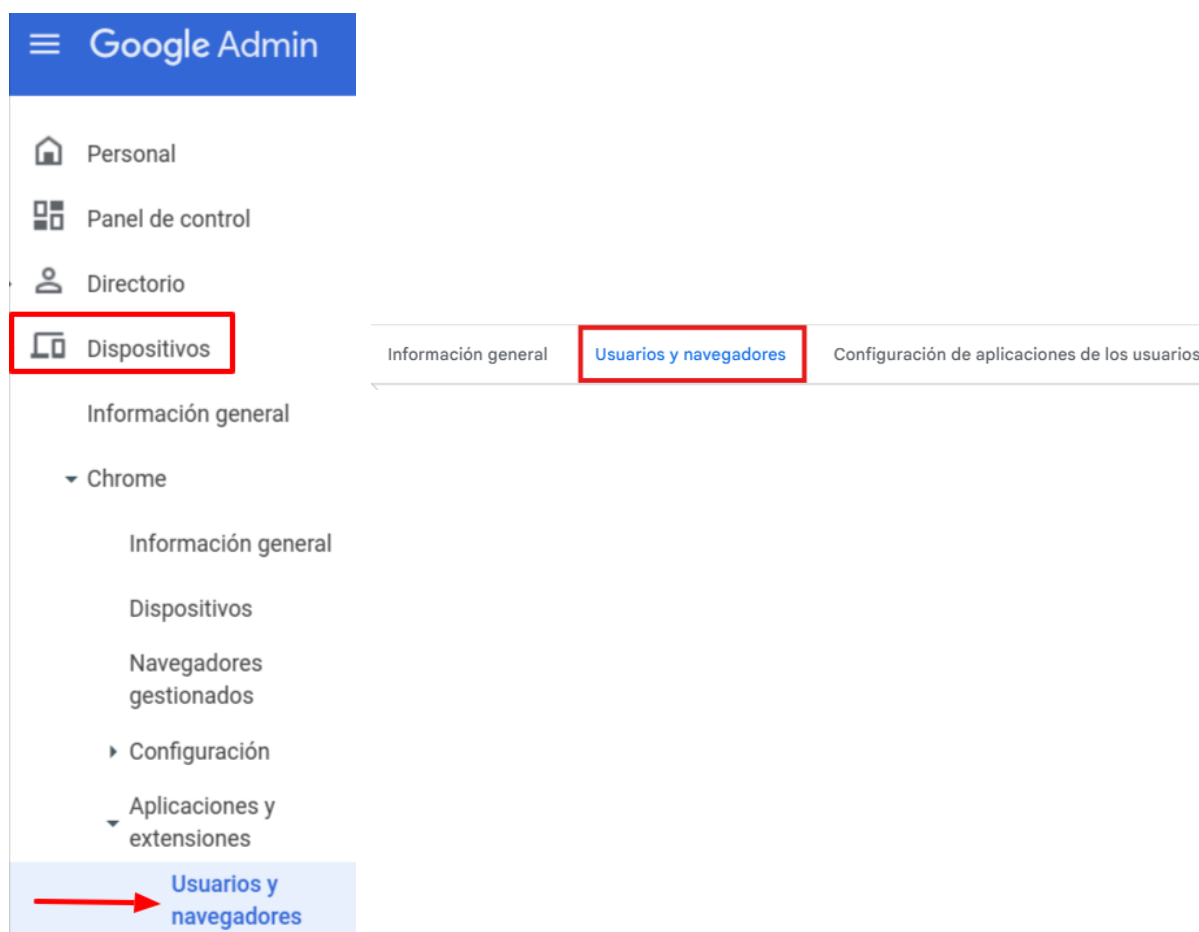
1. Instalación de la extensión IMTLazarus:	2
2. Impedir iniciar sesión con otras cuentas fuera del dominio y modo incógnito:	5
3. Impedir que los usuarios finalicen procesos con el administrador de tareas de Chrome:	8
4. Permisos de registro de los equipos:	8
5. Impedir iniciar sesión como invitado:	9
6. Impedir modo desarrollador:	10
7. Desactivar la ejecución de javascript en la barra del navegador:	11
8. Configurar Geolocalización en Workspace:	12
9. Deshabilitar la Sincronización de Chrome:	13

Introducción

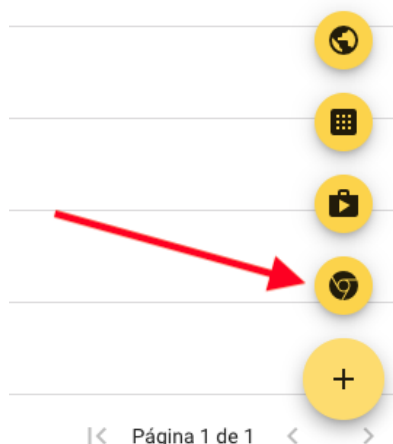
Para que IMTLazarus funcione correctamente en los dispositivos Chrome, IMTLazarus recomienda realizar las siguientes actuaciones dentro de la [Consola de Administración de Google Workspace](#). El primer punto es obligatorio para que IMTLazarus funcione; los siguientes son recomendables para que los usuarios no puedan saltarse el filtrado.

1. Instalación de la extensión IMTLazarus:

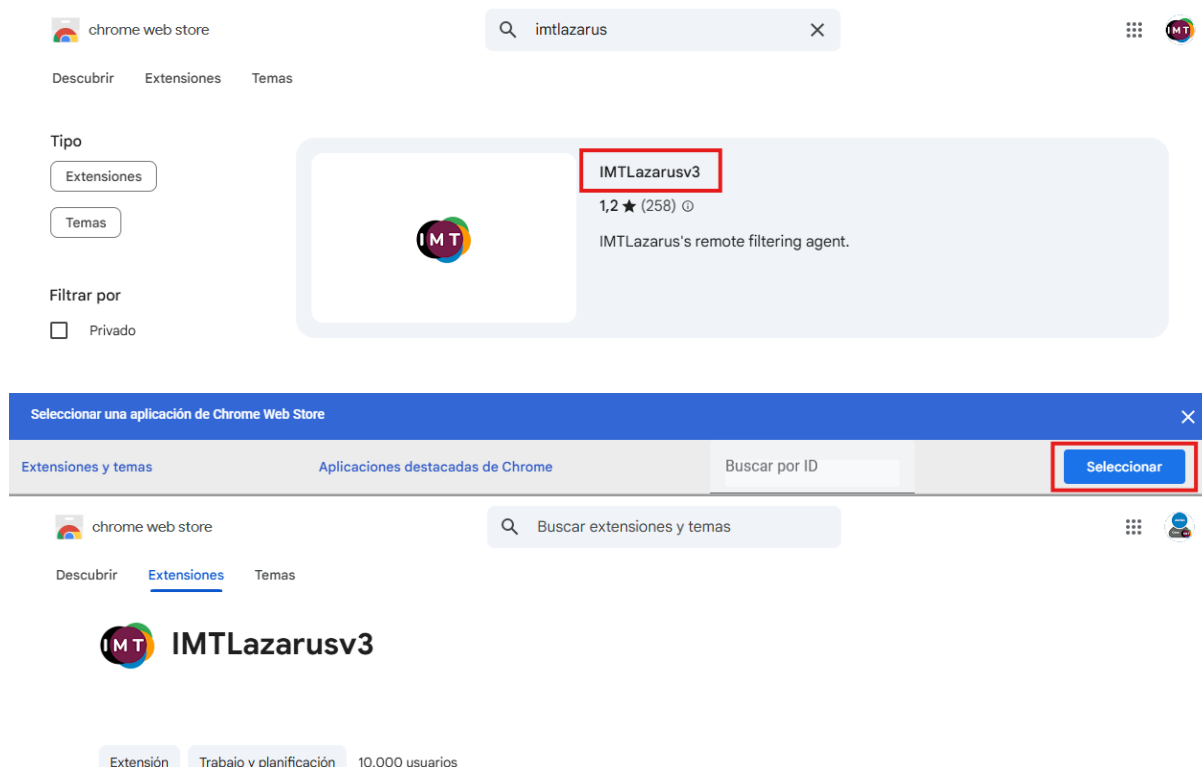
Desde la Consola de Administración de Google Workspace, en el menú de la izquierda, desplegamos el menú Dispositivos > Chrome > Dispositivos Chrome Aplicaciones y extensiones y pinchamos en Usuarios y navegadores:



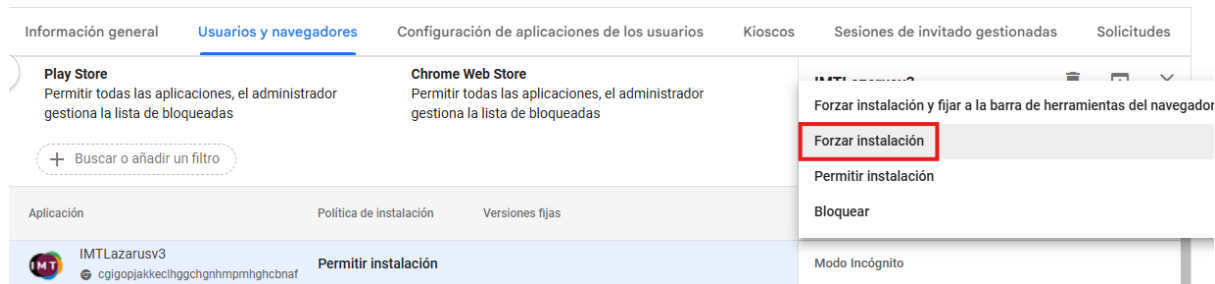
Una vez en esta pantalla, en la parte de la izquierda de la pantalla, seleccionaremos la Unidad Organizativa sobre la que queremos trabajar y, dentro de la pestaña de USUARIOS Y NAVEGADORES, le daremos al botón “+” amarillo que encontraremos abajo a la derecha y luego al icono de Chrome:



Esto hará que se nos abra una nueva ventana llamada “Seleccionar una aplicación de Chrome Web Store” desde la que tendremos que buscar la extensión “IMTLazarusv3”, pinchar sobre ella y después en el botón azul de “Seleccionar”:

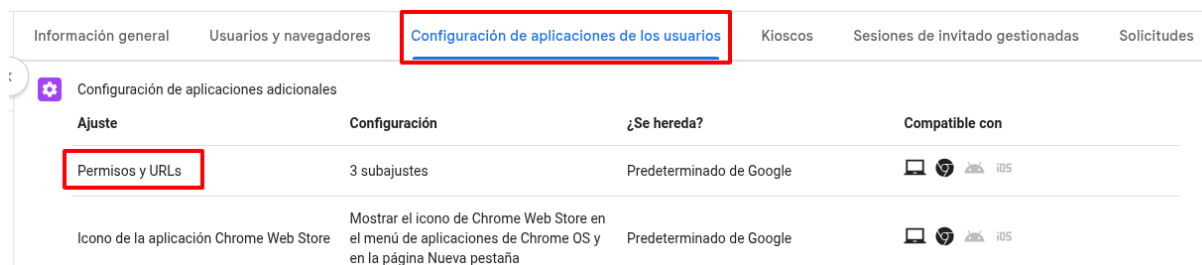


Una vez tengamos disponible la extensión, verificaremos que hemos seleccionado la Unidad Organizativa correcta y seleccionaremos como Política de instalación “Forzar la instalación” y le daremos al botón de “GUARDAR” que nos aparecerá arriba a la derecha de la pantalla.



En el caso de tener instalada una versión anterior de la extensión de IMTLazarus, elimine dicha versión desde esta misma pantalla:

Sin salir de esa pantalla, pinchamos en la pestaña “Configuración de aplicaciones de los usuarios”, en la sección “Configuración de aplicaciones adicionales” hacemos clic en el ajuste “Permisos y URLs”:



Comprobamos que NO tenemos bloqueados los siguientes parámetros:

- Captura de Escritorio
- Bloquear solicitudes web
- Solicitudes web

2. Impedir iniciar sesión con otras cuentas fuera del dominio y modo incógnito:

Desde la Consola de Administración de Google Workspace, en el menú de la izquierda, desplegamos el menú Dispositivos > Chrome > Configuración y pinchamos en Usuarios y navegadores.

Una vez en esta pantalla, en la parte de la izquierda de la pantalla, seleccionaremos la Unidad Organizativa sobre la que queremos trabajar.

Dentro de la pestaña de CONFIGURACIÓN DE USUARIO Y NAVEGADOR, iremos a la sección Experiencia de usuario y en Iniciar sesión en cuentas secundarias tendremos que pinchar y seleccionar la opción “Impedir que los usuarios inicien o cierren sesión en cuentas de Google secundarias”. Para aplicar los cambios, le daremos al botón de “GUARDAR” que nos aparecerá arriba a la derecha de la pantalla.

Configuración de usuarios y navegadores
Configuración del dispositivo
Configuración de sesiones de invitado gestionadas

Mostrar: Todo
+ Buscar o añadir un filtro
Cambios recientes

Experiencia de usuario			
Ajuste	Configuración	¿Se hereda?	Compatible con
Iniciar sesión en cuentas secundarias	2 subajustes	Predeterminado de Google	

Permitir que los usuarios inicien sesión en cualquier cuenta de Google secundaria
Permitir que los usuarios solo inicien sesión en los dominios de Google Workspace especificados abajo
Impedir que los usuarios inicien o cierren sesión en cuentas de Google secundarias

Sin salir de esa pantalla, en la sección “Administración de Chrome para usuarios que han iniciado sesión”, dentro de Administración de Chrome para usuarios que han iniciado sesión seleccionaremos la opción “Aplicar todas las políticas del usuario cuando los usuarios inicien sesión en Chrome y proporcionar una experiencia gestionada de Chrome”.

Administración de Chrome para usuarios que han iniciado sesión ⓘ			
Ajuste	Configuración	¿Se hereda?	Compatible con
Administración de Chrome para usuarios que han iniciado sesión	Aplicar todas las políticas de usuarios cuando se inicia sesión en Chrome y proporcionar una experiencia de Chrome gestionada	Heredado	  

En la sección de “Batería y apagado” y en Configuración de inactividad, dentro de “Bloquear pantalla en caso de suspensión o cierre de la tapa” seleccionaremos la opción de “Bloquear pantalla”:

Configuración	Acción al cerrar la tapa Se ha cerrado la sesión ▼ Bloquear pantalla en caso de suspensión o cierre de la tapa Bloquear pantalla ▼ En versión anteriores a Chrome 106, solo se activa el bloqueo con la suspensión. En Chrome 106 y versiones posteriores, la suspensión o el cierre de la tapa activan el bloqueo. Acción por inactividad con alimentación de CA Se ha cerrado la sesión ▼
---------------	--

En la sección de “Seguridad”, en Modo de incógnito seleccionaremos la opción “No permitir el modo de incógnito” y le daremos al botón de “GUARDAR” que nos aparecerá arriba a la derecha de la pantalla:

Seguridad			
Ajuste	Configuración	¿Se hereda?	Compatible con
Modo Incógnito	No permitir el modo Incógnito	Aplicado de forma local	  

Sin salir de donde estamos en la pestaña de CONFIGURACIÓN DE USUARIO Y NAVEGADOR, iremos a la sección Experiencia de usuario y en Acceso mediante inicio de sesión múltiple seleccionaremos la opción “Bloquear el acceso mediante inicio de sesión múltiple para usuario de esta organización” y le daremos al botón de “GUARDAR” que nos aparecerá arriba a la derecha de la pantalla.

 Experiencia de usuario			
Ajuste	Configuración	¿Se hereda?	Compatible con
Acceso mediante inicio de sesión múltiple	Bloquear el acceso mediante inicio de sesión múltiple para los usuarios de esta organización	Aplicado de forma local	   

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

Sin salir de la pestaña de CONFIGURACIÓN DE USUARIO Y NAVEGADOR, iremos a la sección Aplicaciones y extensiones y en Administrador de tareas seleccionaremos la opción “Impedir que los usuarios finalicen procesos con el administrador de tareas de Chrome” y le daremos al botón de “GUARDAR” que nos aparecerá arriba a la derecha de la pantalla.

 Aplicaciones y extensiones 

Ajuste	Configuración	¿Se hereda?	Compatible con
Administrador de tareas	Impedir que los usuarios finalicen procesos con el administrador de tareas de Chrome	Aplicado de forma local	  

4. Permisos de registro de los equipos:

Para evitar que los usuarios reestablezcan los dispositivos a el estado de fábrica y, por tanto, desinstalen IMTLazarus y cualquier otra aplicación, es necesario que activemos el registro obligatorio del equipo, para que así, si esto ocurriese (el reseteo o “powerwash” del dispositivo Chrome), obligue a enrolarlo en la Consola de Administración para poder utilizarlo.

Para ello, en la Consola de Administración de Google Workspace, en el menú de la izquierda, desplegamos el menú Dispositivos > Chrome > Configuración y pinchamos en Usuarios y navegadores.

Una vez en esta pantalla, en la parte de la izquierda de la pantalla, seleccionaremos la Unidad Organizativa sobre la que queremos trabajar.

Dentro de esta pestaña de CONFIGURACIÓN DE USUARIO Y NAVEGADOR, iremos a la sección Controles de registro, configura el ajuste Permisos de registro como: No permitir que los usuarios de esta organización registren dispositivos nuevos o que ya hayan estado registrados anteriormente.

Le daremos al botón de “Guardar” que aparecerá en la parte superior derecha de la pantalla.

Sin salir de donde estamos, en la pestaña de CONFIGURACIÓN DEL DISPOSITIVO, iremos a la sección Registro y acceso y marcaremos lo siguiente:

- Obligación de volver a realizar el registro: Forzar la repetición del registro del dispositivo con las credenciales del usuario cuando se borren sus datos
- Powerwash: No permitir que se active la función Powerwash

Registro y acceso

Ajuste	Configuración	¿Se hereda?	Compatible con
Obligación de volver a realizar el registro	Forzar la repetición automática del registro del dispositivo cuando se borren sus datos	Predeterminado de Google	   iOS
Entrada del identificador de recursos después de la activación automática	No permitir que se introduzcan el ID ni la ubicación del recurso en los dispositivos que se hayan registrado mediante la activación automática	Predeterminado de Google	   iOS
Powerwash	No permitir que se active la función Powerwash	Aplicado de forma local	   iOS

Le daremos al botón de “Guardar” que aparecerá en la parte superior derecha de la pantalla.

De esta forma, si un usuario restablece los valores de fábrica, tendrá que devolvernos el dispositivo para que lo volvamos a enrolar manualmente con una cuenta de Administrador.

5. Impedir iniciar sesión como invitado:

Desde la misma ventana, pulsaremos en la pestaña de CONFIGURACIÓN DEL DISPOSITIVO, iremos a la sección Configuración de inicio de sesión y en Modo invitados seleccionaremos la opción “Inhabilitar el modo invitados” y le daremos al botón de “GUARDAR” que nos aparecerá arriba a la derecha de la pantalla.

Configuración de inicio de sesión ⓘ

Ajuste	Configuración	¿Se hereda?	Compatible con
Modo Invitado	Inhabilitar el modo Invitado	Aplicado de forma local	   iOS

Si nos hemos salido de la pantalla, podremos volver a la pantalla principal de la Consola de Administración y, en el menú de la izquierda, desplegamos el menú Dispositivos > Chrome > Configuración y pinchamos en Dispositivo.

Seleccionaremos la Unidad Organizativa donde queremos aplicar los cambios. Buscamos la sección llamada Configuración de inicio de sesión y en el parámetro “Modo invitados” marcamos “Inhabilitar el modo invitados”. Para guardar los cambios, le daremos al botón de Guardar que nos aparecerá arriba a la derecha de la pantalla.

6. Impedir modo desarrollador:

Desde la Consola de Administración de Google Workspace, en el menú de la izquierda, desplegamos el menú Dispositivos > Chrome > Configuración y pinchamos en Usuarios y navegadores.

Una vez en esta pantalla, en la parte de la izquierda de la pantalla, seleccionaremos la Unidad Organizativa sobre la que queremos trabajar.

Buscamos la sección llamada Experiencia de usuario y en el parámetro “Herramientas de desarrollo” seleccionamos “No permitir nunca el uso de herramientas de desarrollo integradas”. Para guardar los cambios, le daremos al botón de Guardar que nos aparecerá arriba a la derecha de la pantalla:

Configuración

Disponibilidad de las herramientas de desarrollo

No permitir nunca el uso de herramientas de desarrollo integradas

Modo Desarrollador de la página de extensiones

No permitir el uso de herramientas de desarrollo en la página de extensiones ▼

7. Desactivar la ejecución de javascript en la barra del navegador:

Para prevenir que los alumnos puedan hacer uso de expresiones javascript para intentar saltarse el bloqueo, debemos añadir una configuración adicional.

Desde la Consola de Administración de Google Workspace, en el menú de la izquierda, desplegamos el menú Dispositivos > Chrome > Configuración y pinchamos en Usuarios y navegadores. Seleccionamos la Unidad Organizativa donde queramos aplicar la restricción.

En Bloqueo de URLs añadimos javascript:/* y pulsamos GUARDAR en la parte superior.

Configuración

URLs bloqueadas
javascript:/*

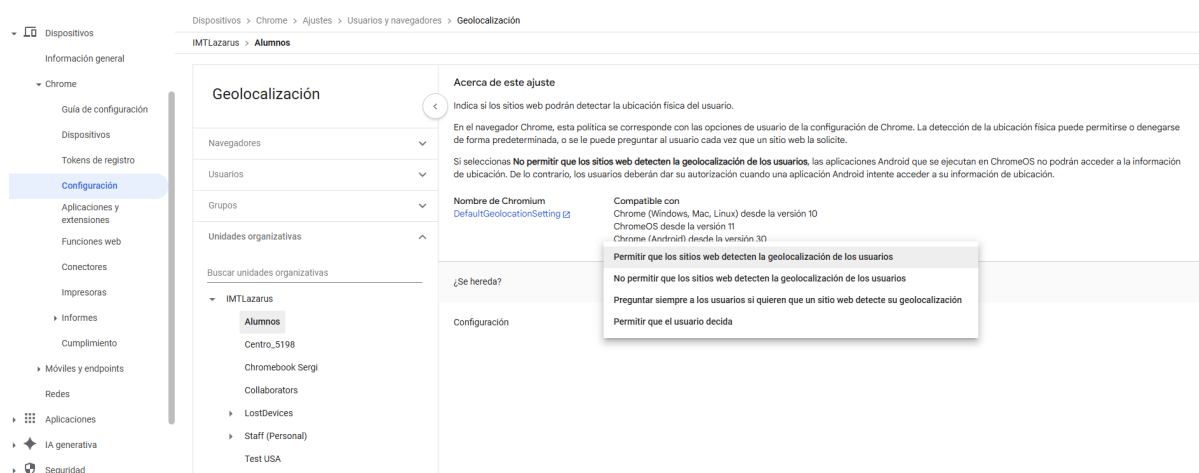
Máximo de 1000 URLs en la lista de bloqueadas. Introduce cada URL en una línea diferente. Por ejemplo:
example.org
https://example.com

8. Configurar Geolocalización en Workspace:

Para garantizar la Geolocalización de los dispositivos debemos configurar el siguiente parámetro en Google Workspace:

Desde el menú de la izquierda, desplegamos el menú Dispositivos > Chrome > Configuración y pinchamos en Usuarios y navegadores. Seleccionamos la Unidad Organizativa donde queramos aplicar la configuración.

En la sección de Seguridad, dentro del parámetro “Geolocalización” seleccionamos la opción “Permitir que los sitios web detecten la geolocalización de los usuarios”



Dispositivos > Chrome > Ajustes > Usuarios y navegadores > Geolocalización

IMTLazarus > Alumnos

Geolocalización

Acerca de este ajuste

Indica si los sitios web podrán detectar la ubicación física del usuario.

En el navegador Chrome, esta política se corresponde con las opciones de usuario de la configuración de Chrome. La detección de la ubicación física puede permitirse o denegarse de forma predeterminada, o se le puede preguntar al usuario cada vez que un sitio web la solicite.

Si seleccionas **No permitir que los sitios web detecten la geolocalización de los usuarios**, las aplicaciones Android que se ejecutan en ChromeOS no podrán acceder a la información de ubicación. De lo contrario, los usuarios deberán dar su autorización cuando una aplicación Android intente acceder a su información de ubicación.

Nombre de Chromium: [DefaultGeolocationSetting](#)

Compatible con:

- Chrome (Windows, Mac, Linux) desde la versión 10
- ChromeOS desde la versión 11
- Chrome (Android) desde la versión 30

Permitir que los sitios web detecten la geolocalización de los usuarios

No permitir que los sitios web detecten la geolocalización de los usuarios

Preguntar siempre a los usuarios si quieren que un sitio web detecte su geolocalización

Permitir que el usuario decida

Y por último pulsamos GUARDAR, arriba a la derecha de la pantalla.

9. Deshabilitar la Sincronización de Chrome:

Para prevenir que los alumnos deshabiliten la extensión, tenemos que apagar la sincronización de Chrome desde la Consola.

Desde el menú de la izquierda, desplegamos el menú Aplicaciones > Servicios adicionales de Google > Configuración de Sincronización de Chrome. Seleccionamos la Unidad Organizativa donde queramos aplicar la configuración y seleccionamos la opción de “Desactivado para todos”.

Aplicaciones > Servicios adicionales de Google > Configuración de Sincronización de Chrome > Estado del servicio



Sincronización de Chrome

Todos los usuarios de esta cuenta

Grupos

Unidades organizativas

Buscar unidades organizativas

IMTLazarus

Alumnos

Mostrando la configuración de los usuarios de Alumnos

Estado del servicio

Estado del servicio

Activado

Desactivado

La mayoría de los cambios se aplicarán en unos minutos. [Más información](#)

HEREDAR