

Gestionar extensiones en una empresa

Gestionar las extensiones de Chrome a gran escala de forma segura

Índice

Objetivo de esta guía

Introducción

Cuestiones que debes tener en cuenta al gestionar extensiones de Chrome

¿Qué son los permisos de las extensiones?

¿Cómo se actualizan las extensiones?

Gestionar las extensiones

Descripción general de las distintas políticas de gestión de extensiones

Bloquear extensiones según sus permisos

Gestionar extensiones según los permisos con Gestión en la nube del navegador Chrome

Gestionar extensiones según los permisos mediante Directiva de grupo

Crear una excepción para extensiones que requieren permisos arriesgados

Gestionar extensiones según la política ExtensionSettings

Configurar la política de extensiones mediante el registro de Windows

Configurar la política de extensiones mediante una cadena JSON en el editor de directivas de grupo de Windows

Impedir que las extensiones modifiquen páginas web

Permitir o bloquear extensiones en la consola de administración de Google

Permitir todas las extensiones excepto las que quieras bloquear

Bloquear todas las extensiones excepto las que quieras permitir

Bloquear o permitir una extensión

Instalación forzada de extensiones

Permitir que los usuarios soliciten extensiones: flujos de trabajo de extensiones

Permitir o bloquear extensiones en Directiva de grupo

Permitir todas las extensiones excepto las que quieras bloquear

Bloquear o permitir una extensión

Forzar la instalación de una extensión

Validar la política

Alojar tus extensiones en servidores propios

Alternativas a alojar las extensiones en servidores propios

Opciones de publicación de extensiones

Fijar una versión concreta de una extensión en la consola de administración

Requisitos para alojar extensiones en servidores propios

Empaquetar la extensión

Alojar la extensión

Publicar actualizaciones para la extensión

Distribuir extensiones alojadas en servidores privados

Gestionar extensiones con Gestión en la nube del navegador Chrome

[Recursos adicionales](#)

Objetivo de esta guía

Hay una gran cantidad de extensiones útiles diseñadas para el navegador Chrome y es posible que muchas se ejecuten en los equipos de tus usuarios. Para los administradores de TI, controlar y supervisar todas estas extensiones puede ser una tarea difícil.

Esta guía está dirigida a los administradores de TI que quieren saber cuáles son las mejores formas de gestionar las extensiones. En ella se describen los pasos para administrarlas mediante [Gestión en la nube del navegador Chrome](#) y con Directiva de grupo de Windows.

La guía está organizada según las formas en que se pueden gestionar las extensiones. Puedes hacer lo siguiente:

1. Bloquear extensiones según sus permisos.
2. Decidir a qué sitios web podrán acceder las extensiones.
3. Permitir o bloquear extensiones en Gestión en la nube del navegador Chrome o mediante Directiva de grupo de Windows.
4. Alojamiento de tus propias extensiones en un servidor local.

Temas tratados	Instrucciones y recomendaciones para gestionar extensiones del navegador Chrome en una empresa
Audiencia principal	Administradores de Microsoft® Windows® y Gestión en la nube del navegador Chrome (disponible para Windows, Mac y Linux)
Datos clave	Prácticas recomendadas para gestionar extensiones del navegador Chrome

Última actualización: 29 de octubre del 2021

Ubicación de la publicación: <https://support.google.com/chrome/a/answer/9296680>

Productos de terceros: en este documento se describe cómo funcionan los productos de Google con los sistemas operativos de Microsoft Windows y las configuraciones que Google recomienda. Google no ofrece asistencia técnica para configurar productos de terceros ni asume responsabilidad alguna por el uso de dichos productos. Para ver la información más reciente sobre configuración y asistencia, consulta el sitio web del producto en cuestión. También puedes ponerte en contacto con los proveedores de soluciones de Google para acceder a servicios de consultoría.

©2021 Google LLC. Todos los derechos reservados. Google y el logotipo de Google son marcas registradas de Google LLC. Los demás nombres de productos y empresas pueden ser marcas de las correspondientes empresas a las que están asociados.
[EXTENSIONS-en-1.0]

Introducción

Para proteger los datos de sus usuarios, las empresas necesitan poder comprobar fácilmente que las extensiones son seguras y útiles. Los administradores de TI necesitan hacer lo siguiente:

1. Impedir que se instalen extensiones dañinas.
2. Mantener las extensiones que necesitan los usuarios.
3. Proporcionar acceso limitado a los datos de los usuarios y de la empresa.

El objetivo de esta guía es mostrarte cómo puedes gestionar las extensiones fácilmente. Existen diferentes métodos para gestionar extensiones. En esta guía describimos las diferentes opciones y te ayudamos a elegir el método más adecuado para tu caso concreto.

Cuestiones que debes tener en cuenta al gestionar extensiones de Chrome

Para poder hacer su trabajo, tus usuarios necesitan acceder a determinados sitios, aplicaciones y extensiones. Por otro lado, como administrador de TI, eres responsable de proteger los datos de los usuarios y de la empresa. Para elegir la forma más adecuada de gestionar las extensiones, deberás definir una estrategia.

Estas son las preguntas principales que debes hacerte a la hora de elegir tu estrategia:

- ¿A qué normativas y medidas sobre cumplimiento está sujeta mi empresa?
- ¿Qué tipo de acceso a través de un dispositivo o un sitio web podría infringir las políticas de seguridad de mi empresa?
- ¿Qué volumen de datos propios o de la empresa se almacena en los equipos de mis usuarios?

Cualesquiera que sean las decisiones que tomes, Google te proporciona políticas con las que puedes hacer lo siguiente:

- Bloquear o permitir extensiones conforme a tus políticas de protección de datos.
- Instalar de manera forzada las extensiones necesarias en los equipos de tus usuarios.
- Gestionar extensiones y concederles el nivel mínimo de derechos necesarios para que puedan funcionar.

El modelo de gestión convencional consiste en permitir o bloquear extensiones concretas. Sin embargo, existe un método más sencillo: puedes gestionar las extensiones según los permisos que necesitan. Para ello, primero debes decidir qué permisos vas a conceder y, a continuación, aplicar políticas que permitan o bloqueen las extensiones, según los permisos que hayas definido.

¿Qué son los permisos de las extensiones?

Las extensiones pueden necesitar ciertos derechos para hacer cambios en un equipo o una página web con el fin de ejecutarse correctamente. Estos derechos se denominan "permisos". Los desarrolladores deben elaborar listas de los derechos y niveles de acceso que requieren sus extensiones. Aunque existen dos categorías principales de permisos, muchas extensiones tienen ambas:

- Los permisos de sitios permiten acceder a los sitios web que visitan tus usuarios.
Ejemplos: modificar una página web, acceder a las cookies o modificar pestañas.
- Los permisos de dispositivos permiten acceder al equipo en el que se ejecuta el navegador.
Ejemplos: acceder a un puerto USB, almacenar contenido o ver la pantalla.

¿Cómo se actualizan las extensiones?

Las extensiones solo se actualizan cuando Chrome se está ejecutando. El proceso se lleva a cabo durante los cinco primeros minutos después de abrir Chrome y, posteriormente, cada cinco horas.

- El proceso de actualización de las extensiones tiene lugar de esta forma:
 - a. Chrome envía a un servidor de Google una solicitud que contiene una lista de versiones y extensiones instaladas.
 - b. Nuestros servidores responden enviando una serie de instrucciones sobre qué extensiones se deben actualizar.
 - c. A continuación, Chrome solicita los archivos CRX de cada extensión obsoleta y aplica la actualización de forma local.
- Cómo se pueden quedar obsoletas las extensiones:
 - a. Cuando el tamaño de la descarga de la actualización es muy grande o si los usuarios tienen muchas extensiones, es posible que la actualización no se complete si la sesión de usuario es corta.
 - b. Si no se abre Chrome.
 - c. Si los desarrolladores de extensiones han decidido limitar la cantidad de clientes en los que implementan una actualización.
 - d. Si una empresa aloja una extensión en sus servidores, las extensiones se podrían quedar obsoletas debido a un problema de acceso o un error de configuración.
 - e. Debido a otros problemas asociados a errores en el diseño de la extensión.

Para solucionar el problema de una extensión obsoleta, se puede desinstalar y volver a instalar la extensión, o actualizarla automáticamente en `chrome://extensions > habilitar modo desarrollador > hacer clic en el botón Actualizar`.

Gestionar las extensiones

La mayoría de las organizaciones deberían gestionar las extensiones según los permisos y los sitios web a los que tienen acceso. Este método es más seguro, sencillo y escalable.

Además, te permitirá ahorrar tiempo, ya que solo tendrás que definir las políticas una vez. De esta forma, ya no necesitarás gestionar largas listas de extensiones permitidas y bloqueadas. Sin embargo, si lo consideras conveniente, puedes crear una pequeña lista de extensiones bloqueadas que los usuarios no podrán instalar. Además, con la política de hosts en tiempo de ejecución, tus sitios más importantes estarán protegidos. Para gestionar las extensiones de tu organización con este método:

1. Averigua qué extensiones están instaladas en los ordenadores de tus usuarios.
 - **Método 1 (recomendado):** usa [Gestión en la nube del navegador Chrome](#). Esta función está disponible para tus usuarios sin ningún coste adicional. Podrás ver esta información sobre la extensión:
 - La versión actual, el número de veces que se instaló y si la instaló el usuario o un administrador
 - Los permisos que requiere
 - Su estado (activa o inhabilitada)
 - Consulta los pasos para configurar Gestión en la nube del navegador Chrome [aquí](#).

- Una vez que hayas configurado la consola y registrado los equipos con los informes en la nube habilitados, podrás ver todas las extensiones instaladas en **Dispositivos > Chrome > Informe de uso de aplicaciones y extensiones**.
 - Al hacer clic en una extensión, se mostrarán algunos datos más sobre los permisos que requiere y ejemplos de dónde está instalada.
 - A partir de finales del 2021 o principios del 2022, cuando hagas clic en una extensión, se te dirigirá a la nueva página de detalles de la extensión (consulta la imagen más abajo).
 - Allí podrás ver más información, como los permisos que requiere y datos obtenidos directamente de las fichas de Chrome Web Store.
 - Para obtener más información sobre cómo gestionar extensiones en Gestión en la nube del navegador Chrome, echa un vistazo a este [vídeo de YouTube](#).
 - También puedes usar la API de Takeout de Gestión en la nube del navegador Chrome para exportar a un archivo CSV todos los datos de extensiones instaladas en navegadores registrados.
 - Para obtener más información, consulta: [Guía detallada](#) | [Entrada de blog](#) | [Vídeo de demostración](#)
- **Método 2 (encuesta)**: pregunta a tus colaboradores y a sus administradores qué extensiones utilizan habitualmente. Crea una lista con las extensiones que necesitan los usuarios.

2. Decide qué sitios debes proteger:
 - Decide en qué sitios web o dominios con información sensible no podrán hacer cambios ni leer datos las extensiones.
 - Para impedir que accedan a estos sitios, deberás bloquear las llamadas a la API cuando se ejecute la extensión. De esta forma, se bloquearán las solicitudes web, la lectura de cookies, la inserción de JavaScript, las solicitudes XHR, etc.
3. Identifica qué permisos podrían implicar riesgos para tus usuarios:
 - Revisa la lista de extensiones que creaste en el paso 1. Revisa las extensiones que están instaladas y averigua qué permisos requieren.
 - **Consejo:** Los permisos que utilizan las extensiones pueden ser demasiado generales. Ponte en contacto con el proveedor de las extensiones que necesiten tus usuarios para solicitar más información. Podrá explicarte qué cambios podría hacer la extensión en los equipos y en los sitios web.
 - Examina la [lista Declare Permissions](#) (Declarar permisos). En esta lista se indican todos los permisos que puede usar una extensión. Después, decide qué permisos quieres autorizar en tu organización.
 - Consulta [este documento sobre los riesgos de los permisos de aplicaciones específicas](#).
4. Con los datos que has recogido, crea una lista en la que se incluya la información que se indica a continuación.
 - **Extensiones requeridas:** esta lista se podría desglosar por departamento, ubicación de la oficina u otra información relevante.
 - **Lista de extensiones permitidas:** las extensiones requeridas con los permisos que se bloquearían, pero que se deben permitir para que las extensiones funcionen. Ejemplos:
 - Extensiones que tus usuarios necesitan.
 - Extensiones que, según te ha indicado el proveedor, no implican ningún riesgo.
 - **Lista de extensiones bloqueadas:**
 - Extensiones que los usuarios no podrán instalar.
 - En esta lista se incluyen los permisos que no se podrán usar.
 - Se incluyen los sitios web y dominios que se deben proteger y a los que las extensiones no podrán acceder.
 - Compara esta lista de extensiones bloqueadas con otras listas que tengas. Es posible que descubras que puedes relajar tus políticas sobre listas de elementos bloqueados.
5. Facilita la lista a tus colaboradores y al equipo de TI para que la aprueben.
6. Prueba la nueva política en tu laboratorio o realiza una prueba piloto con un grupo pequeño de usuarios de tu organización.
7. Despliega estos nuevos conjuntos de políticas en las cuentas de los empleados por fases.
8. Revisa los comentarios de tus usuarios.
9. Repite el proceso una vez al mes, al trimestre o al año y realiza las correcciones oportunas.

De esta forma, tendrás una base de los permisos que admites y podrás bloquear todos los demás. Los sitios web con contenido sensible estarán protegidos. La seguridad del navegador aumentará y la experiencia de usuario será mejor. Los empleados podrían instalar extensiones que antes no estaban permitidas. En tus sitios web con información sensible, las extensiones no funcionarán, a menos que lo permitas. Si quieres saber cuáles son los pasos para configurar este método, consulta los siguientes temas de esta guía:

- [Gestionar extensiones bloqueando o admitiendo permisos](#)
- [Hosts bloqueados en tiempo de ejecución](#) (proteger sitios web con información sensible)
- [Instalar extensiones de manera forzada](#) en las cuentas de tus usuarios
- [Permitir o bloquear extensiones \(si fuera necesario\)](#)

Para ver información general sobre cómo gestionar extensiones en Gestión en la nube del navegador Chrome, echa un vistazo a este [vídeo de YouTube en el que se explica cómo gestionar extensiones en la consola de administración](#).

Descripción general de las distintas políticas de gestión de extensiones

Aunque muchas de estas políticas se abordan en detalle en las otras secciones de esta guía, a continuación te mostramos un resumen de algunas de las opciones que tienes para gestionar extensiones (algunas también sirven para gestionar aplicaciones) a través de Directiva de grupo de Windows o de archivos .plist en Mac:

- [ExtensionInstallAllowlist](#): extensiones que has autorizado para que se instalen en tu entorno.
- [ExtensionInstallBlocklist](#): extensiones que no permites que se instalen. Si ya están instaladas, se inhabilitarán. Si un usuario intenta instalar una de estas extensiones, la instalación se bloqueará. Asimismo, una nueva función de Chrome Web Store muestra el botón "Añadir a Chrome" en rojo e indica al usuario que no se autoriza la instalación de la extensión.
- [ExtensionInstallForcelist](#): con esta política, la extensión se instalará de forma silenciosa en el equipo del usuario, que no podrá inhabilitarla ni desinstalarla. Este ajuste prevalece sobre la política de lista de extensiones bloqueadas.
- [BlockExternalExtensions](#): este ajuste impedirá que se instalen extensiones de fuentes externas. Por ejemplo, si una aplicación instalada añade una extensión a Chrome a través del registro, este ajuste impedirá que se cargue la extensión.
- [ExtensionAllowedTypes](#): te permite crear una lista de los tipos de extensiones y aplicaciones que podrán instalar tus usuarios. Puedes indicar extensiones, temas, secuencias de comandos de usuario, aplicaciones alojadas, aplicaciones empaquetadas antiguas y aplicaciones de plataformas.
 - Ten en cuenta que deberás incluir en la lista todos aquellos elementos que quieras permitir. No se podrá instalar nada que no esté incluido en la lista.
 - Consulta más información sobre las [extensiones y aplicaciones de Chrome Web Store](#).
- [ExtensionInstallSources](#): en las versiones anteriores, los usuarios podían hacer clic en un enlace a un archivo .crx y Chrome les ofrecía la opción de instalar la extensión después de mostrar algunas advertencias. Esta función se eliminó por motivos de seguridad en las versiones posteriores a Chrome 21.
 - Esta política te permite utilizar esta función antigua en las URLs específicas que indiques. Consulta los [patrones de coincidencia de URLs](#) que se pueden usar en esta política.

- [ExtensionsSettings](#): esta política, que proporciona distintas funciones, requiere que se cree una secuencia de comandos JSON en una cadena de una sola línea.
 - Este ajuste puede ser complejo y se abordará en detalle en distintas secciones de esta guía.
 - Te recomendamos que consideres la opción de usar Gestión en la nube del navegador Chrome, ya que incluye casi todas las funciones sin tener que escribir un archivo JSON y, además, permite supervisar las extensiones instaladas.

Una observación sobre el compromiso de Google de utilizar convenciones de nomenclatura inclusivas. Las siguientes políticas están obsoletas y se eliminarán en Chrome 97, por lo que debes empezar a usar las políticas nuevas a partir de dicha versión.

- [ExtensionInstallWhitelist](#) se ha sustituido por [ExtensionInstallAllowlist](#)
- [ExtensionInstallBlacklist](#) se ha sustituido por [ExtensionInstallBlocklist](#)


Bloquear extensiones según sus permisos

Puedes controlar qué extensiones podrán instalar tus usuarios según los permisos que requieran. Se inhabilitará una extensión instalada cuyos permisos se bloqueen. Si un usuario intenta instalar una extensión cuyos permisos estén bloqueados, la instalación no se llevará a cabo.

Gestionar extensiones según los permisos con Gestión en la nube del navegador Chrome

(Windows, Mac y Linux)

Puedes bloquear extensiones que necesiten permisos no autorizados. Por ejemplo, podrías impedir que las extensiones se conecten a dispositivos USB o que accedan a las cookies.

1. En la consola de administración, ve a **Dispositivos > Chrome > Aplicaciones y extensiones > Usuarios y navegadores**.
2. Selecciona la unidad organizativa donde estén los usuarios para los que quieras permitir las extensiones.
3. Haz clic en el icono de la rueda dentada de Configuración adicional 
4. En la sección **Permisos y URLs**, marca los permisos que quieres bloquear o permitir.

Permisos y URLs
Aplicado de forma local

Bloquear extensiones según los permisos

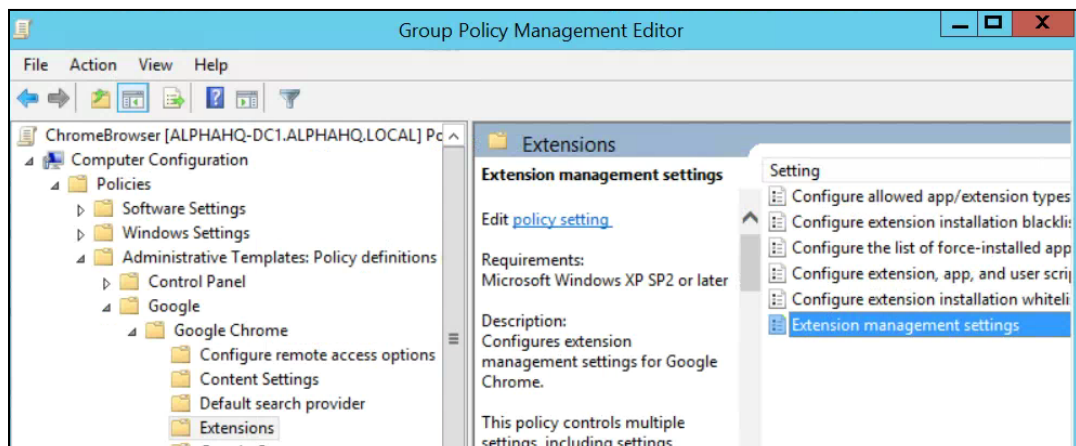
<input type="checkbox"/> Alarmas	<input type="checkbox"/> Captura de audio	<input type="checkbox"/> Proveedor de certificados
<input type="checkbox"/> Lectura del portapapeles	<input type="checkbox"/> Escritura del portapapeles	<input type="checkbox"/> Menús contextuales
<input type="checkbox"/> Captura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

- a. También puedes hacer clic en una extensión individual, en la pestaña Usuarios y navegadores, y gestionar los permisos en Permisos y acceso a través de URL > Personalizar los permisos de esta aplicación/extensión.
 - i. Ten en cuenta que este ajuste anulará cualquier política global que ya se esté aplicando a esta extensión.
 - ii. Para ver información detallada de cada permiso, consulta esta [lista de permisos](#).
5. Haz clic en **Guardar**.

Gestionar extensiones según los permisos mediante Directiva de grupo

(solo en Windows)

1. Desplázate hasta el objeto de directivas de grupo (GPO), en la consola de administración de Microsoft.
2. Haz clic con el botón derecho y, a continuación, haz clic en **Editar**.
3. En el Editor de administración de directivas de grupo, ve a **Directivas > Plantillas administrativas > Google Chrome > Extensiones > Configuración de administración de extensiones**.



Ruta de la Configuración de administración de extensiones

4. Habilita la política y, a continuación, introduce los permisos que quieres permitir o bloquear. Debes comprimirlos en una única cadena JSON.

Aplica el formato tal como se muestra en este ejemplo de datos JSON. En este ejemplo se bloquea cualquier extensión que necesite usar un puerto USB.

```
{
  "*": {
    "blocked_permissions": ["usb"]
  }
}
```

Datos JSON compactos:

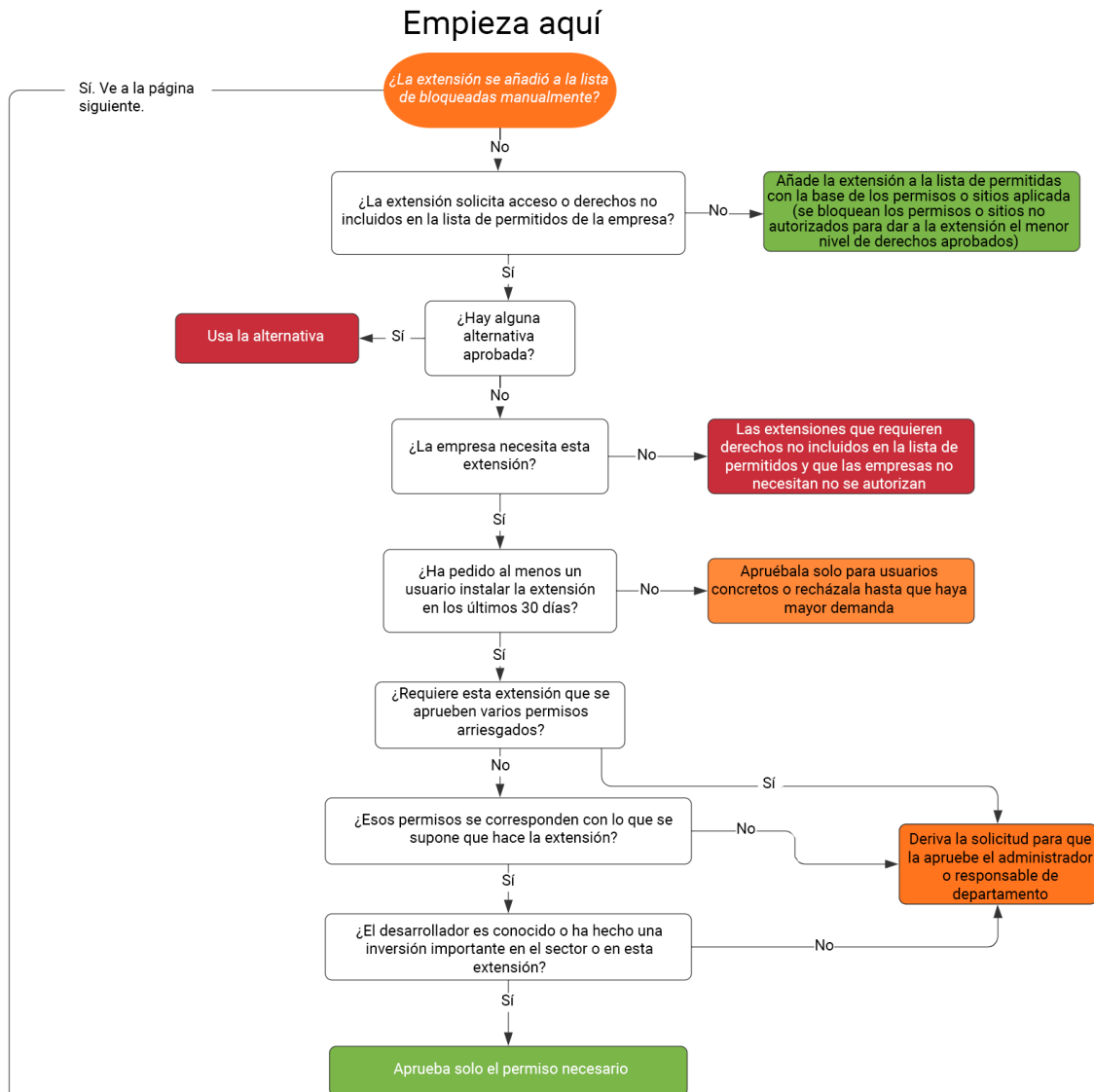
```
{"*":{"blocked_permissions":["usb"]}}
```

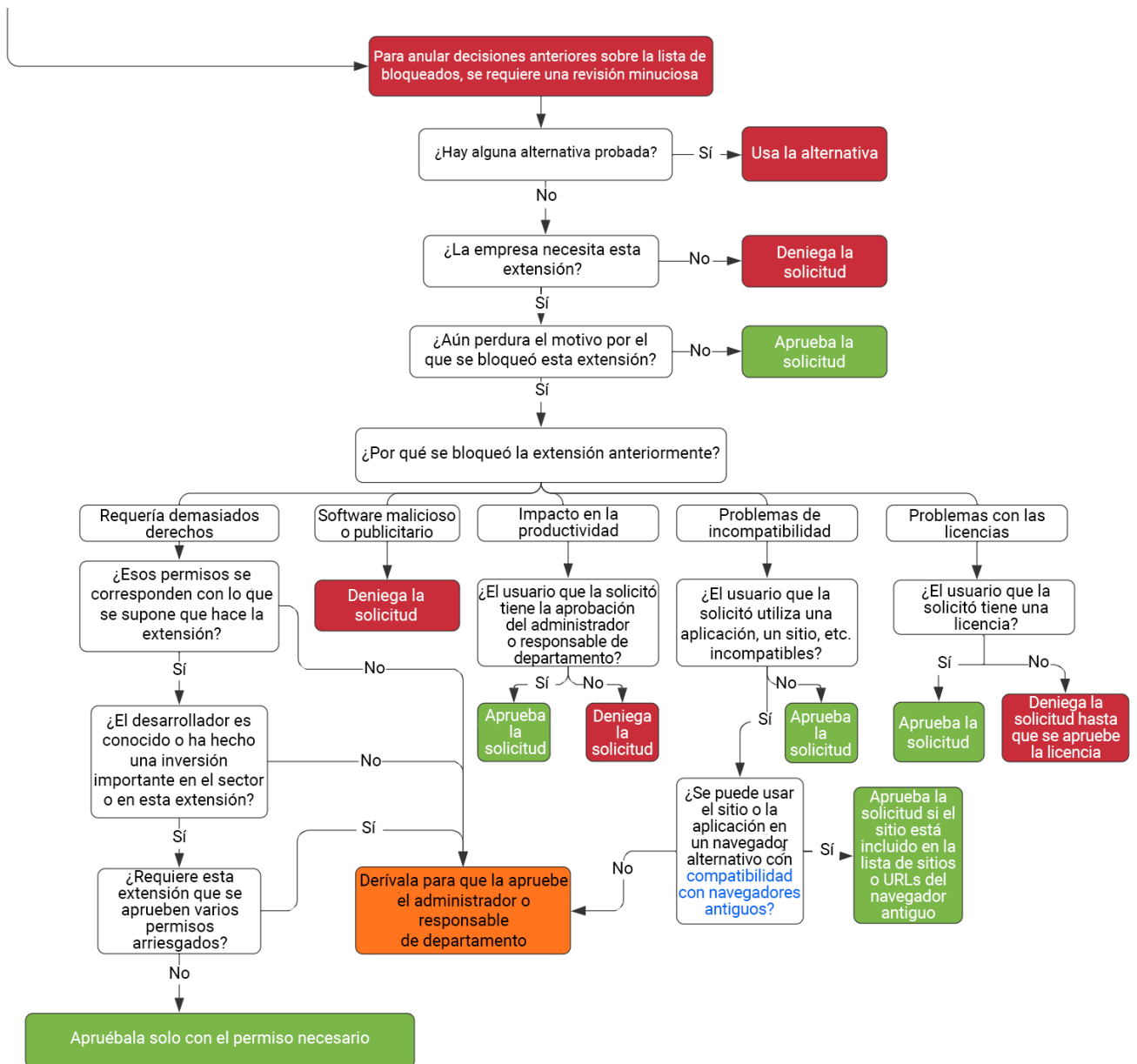
Consejo:

- Para bloquear todas las extensiones que requieren ese permiso, usa un asterisco (tal como se muestra más arriba) como ID de extensión.
- Si quieres bloquear varios permisos a través de JSON, consulta este ejemplo en el que se bloquean los elementos power, printerProvider, serial y usb para todas las extensiones:
 - `{"*":{"blocked_permissions":["power","printerProvider","serial","usb"]}}`
- Si especificas un ID de extensión, la política solo se aplicará a esa extensión. En el ejemplo anterior, sustituye el asterisco (*) por el ID de la extensión. Puedes bloquear más de una extensión, pero cada una deberá tener su propia entrada en la cadena JSON.
 - Para ver instrucciones sobre cómo hallar el ID de una extensión, consulta el paso 3 de [este artículo de ayuda](#).

Crear una excepción para extensiones que requieren permisos arriesgados

Es posible que en tu empresa se requieran extensiones que necesiten permisos que te parezcan demasiado arriesgados para usarlos en tu entorno. Para que te hagas una idea de cómo podría ser el procedimiento para establecer una excepción, te mostramos un ejemplo de una extensión que requiere un permiso que está bloqueado actualmente.





- Ten en cuenta que este procedimiento se ofrece únicamente a modo de ejemplo, ya que cada empresa tendrá su propio método o procesos específicos para la gestión del cambio.

Gestionar extensiones según la política ExtensionSettings

Windows ofrece diferentes formas de gestionar extensiones. Una de las más habituales consiste en definir varias políticas con una cadena JSON o con el registro de Windows utilizando la [política ExtensionSettings](#).

Nota: Esta política se admite en [Mac](#), [Chrome OS](#) y [Linux](#). En la [página de la política](#) se incluyen valores de ejemplo para estas plataformas.

Esta política puede controlar ajustes como la URL de actualización, desde la que se descarga la extensión para la instalación inicial, y los permisos bloqueados, que no se podrán utilizar. Para obtener más información, consulta la [descripción completa de la configuración de la extensión](#). También puedes consultar estos artículos de ayuda: [Configurar la política ExtensionSettings](#) y [Políticas de aplicaciones y extensiones](#).

Puedes definir toda la configuración de la gestión de las extensiones a través de esta política o mediante políticas individuales.

- Los ajustes Hosts permitidos en tiempo de ejecución o Hosts bloqueados en tiempo de ejecución (bloquear extensiones en sitios web específicos) solo se pueden definir mediante GPO dentro de la política ExtensionSettings.
 - También se pueden definir con [Gestión en la nube del navegador Chrome](#).
- Ten en cuenta que la política ExtensionSettings puede anular otras políticas que hayas definido en otro lugar de Directiva de grupo, como:
 - [ExtensionAllowedTypes](#)
 - [ExtensionInstallAllowlist](#)
 - [ExtensionInstallForcelist](#)
 - [ExtensionInstallSources](#)
 - [ExtensionInstallBlocklist](#)

La política ExtensionSettings se define con uno de estos dos métodos:

- [Registro de Windows](#)
- [Cadena JSON en el editor de directivas de grupo de Windows](#)

Consejos:

- Aplicar formato correctamente a una cadena JSON puede ser algo difícil. Usa una herramienta de revisión de JSON antes de implementar la política.
- Si tienes dificultades para aplicar el formato correcto a la cadena JSON, puedes usar el método de la clave de registro. De esta forma, Chrome lo convertirá a JSON dentro de la URL chrome://policy en el navegador del equipo de destino.
 - Solo tienes que copiar esa cadena JSON y aplicarla mediante GPO a través de la política ExtensionSettings.
 - También puedes usar este método configurando la política ExtensionSettings con Gestión en la nube del navegador Chrome y copiando la cadena JSON obtenida.

Configurar la política de extensiones mediante el registro de Windows

La política ExtensionSettings se debe escribir en el registro en esta ubicación:

HKLM\Software\Policies\Google\Chrome\ExtensionSettings\

- Se puede usar HKCU en lugar de HKLM. La ruta equivalente se puede configurar mediante GPO.
- Las claves se pueden crear con el método que prefieras en el equipo del usuario.

En el caso de Chrome, todos los ajustes comienzan con esta clave:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\ExtensionSettings\

La siguiente clave que debes crear se utiliza para el permiso de la política. Si vas a aplicar la clave a una extensión, dale el nombre del ID de la extensión. Si la vas a aplicar a todas las extensiones, dale como nombre un asterisco. Por ejemplo, usa esta ubicación para los ajustes que se apliquen únicamente a la extensión de Google Hangouts:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\ExtensionSettings\nckgahadag
oaajjgafhacjanaoihapd

En el caso de ajustes que se apliquen a todas las extensiones, usa esta ubicación:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\ExtensionSettings*

Diferentes ajustes requerirán distintos formatos, según si se trata de una cadena o de un array de cadenas.

Los valores de array requieren el formato ["value"]. Los valores de cadena se pueden introducir sin [" "].

Lista de ajustes que son arrays o cadenas:

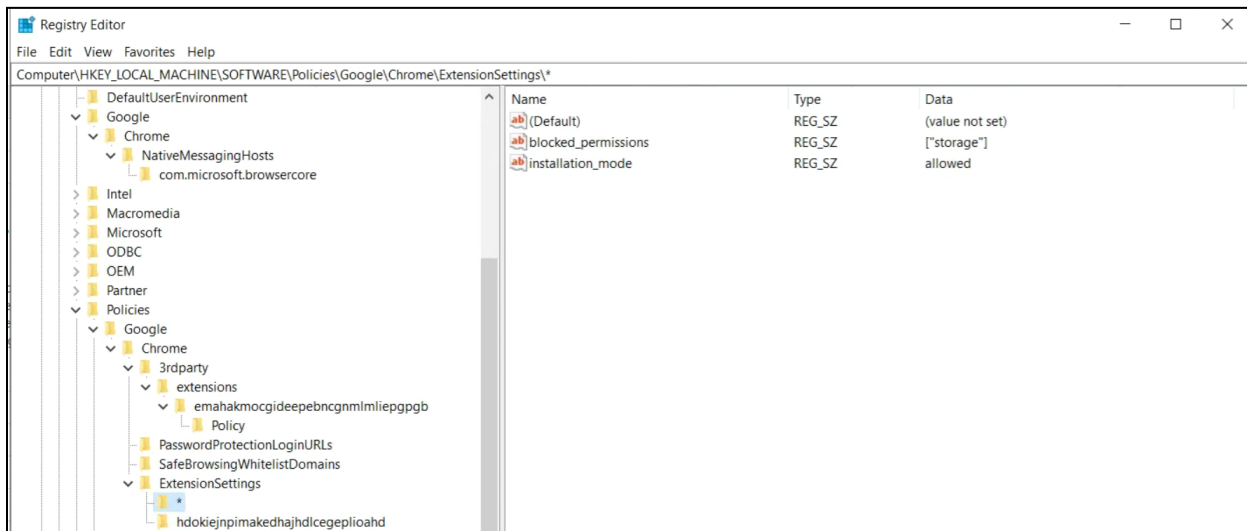
- Installation_mode = cadena
- update_url = cadena
- blocked_permissions = array de cadenas
- allowed_permissions = array de cadenas
- minimum_version_required = cadena
- runtime_blocked_hosts = array de cadenas
- runtime_allowed_hosts = array de cadenas
- blocked_install_message = cadena

Si quieres definir varios valores en una sola cadena (como permisos bloqueados), aquí tienes un ejemplo de esa sintaxis:

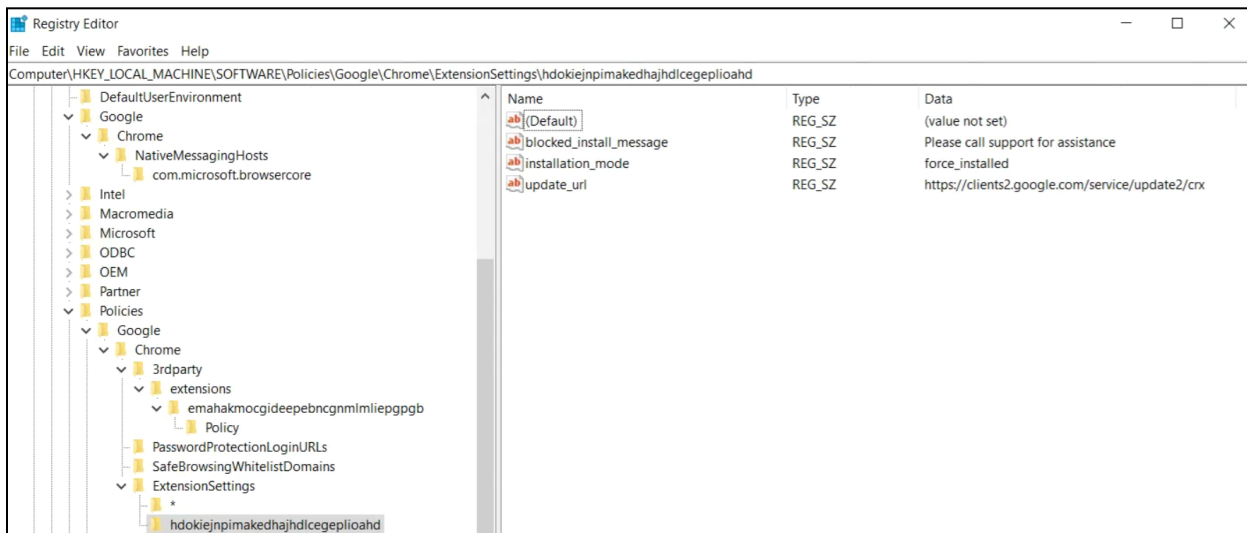
- ["power","printerProvider","serial","usb"]

Name	Type	Data
 (Default)	REG_SZ	(value not set)
 blocked_permissions	REG_SZ	["power", "printerProvider", "serial", "usb"]

Ejemplos del aspecto de las cadenas en el registro:



La clave de permiso predeterminada (*) y sus valores



Un permiso individual y sus valores

En este caso, las claves definidas en el registro se convierten en JSON con la política chrome://policy en el navegador:

Chrome policies

A qué se aplica	Nivel	Fuente	Nombre de la política
Equipo	Obligatoria	Plataforma	DefaultBrowserSettingEnabled
Equipo	Obligatoria	Plataforma	ExtensionSettings

```
{
  "*": {
    "blocked-permissions": [ "storage" ],
    "installation_mode": "allowed"
  },
  "hdokiejnpimakedhajhdicegplioahd": {
    "blocked_install_message": "Please call support for assistance",
    "installation_mode": "force_installed",
    "update_url": "https://clients2.google.com/service/update2/crx"
  }
}
```

Configurar la política de extensiones mediante una cadena JSON en el editor de directivas de grupo de Windows

En el procedimiento donde se indica cómo utilizar la política de configuración de extensiones mediante GPO se presupone que ya has importado las [plantillas ADM o ADMX para políticas de Chrome](#).

Para ver instrucciones de otras plataformas de sistemas operativos, consulta estas referencias: [Mac](#) | [Linux](#) | [Chrome OS](#)

1. En el Editor de administración de directivas de grupo, ve a **Google Chrome > Extensiones > Configuración de administración de extensiones**.
2. Habilita la política y, en el cuadro de texto, escribe los datos de su archivo JavaScript Object Notation (JSON) compacto en una sola línea, sin saltos de línea.
Para validar y compactar políticas en una sola línea (puedes ver un ejemplo de datos JSON más abajo), utiliza esta [herramienta de compresión en formato JSON de terceros](#).

Aplicar el formato JSON correcto para usar la política de configuración de extensiones:

Para utilizar este método, es necesario comprender las dos partes de las que se compone esta política: el permiso **predeterminado** y el permiso **individual**. El permiso predeterminado se aplica a todas las extensiones. El individual se aplica solo a la extensión especificada.

El permiso predeterminado se identifica por medio del asterisco (*). En este ejemplo, se definen un permiso predeterminado y un permiso de extensión individual:

```
{
  "*": {},
  "nckgahadagoaajjgafhacjanaoiihapd": {}
}
```

Una extensión obtiene su configuración solo de un permiso. Si esa extensión tiene un permiso individual, se le aplicará esa configuración. Si no hay ningún permiso individual para la extensión, se utilizará el predeterminado.

A continuación se muestra un ejemplo de JSON que impide que se ejecute cualquier extensión en .example.com y que bloquea todas las extensiones que requieren el permiso "USB":

```
{
  "*": {
    "runtime_blocked_hosts": ["*://*.example.com"],
    "blocked_permissions": ["usb"]
  }
}
```

Datos JSON compactos:

```
{"*":{"runtime_blocked_hosts":["*://*.example.com"],"blocked_permissions":["usb"]}}
```

Ejemplos de referencia con valores de muestra para la gestión de la instalación de extensiones:

- "allowed" (predeterminado)
El usuario puede instalar la extensión desde Chrome Web Store.
Ejemplo de JSON:

```
{ "*": {"installation_mode": "allowed" } }
```
- "blocked"
El usuario no puede instalar la extensión desde Chrome Web Store.
Ejemplo de JSON:

```
{ "*": {"installation_mode": "blocked" } }
```
- "blocked_install_message"
Aquí se puede especificar un mensaje personalizado para que se muestre cuando se bloquee la instalación.
Ejemplo de JSON con blocked_install_message:

```
{"*":{"blocked_install_message":["Llamar a TI (408 - 555 - 1234) para aplicar una excepción"]}}
```
- "force_installed"
 - La extensión se instala automáticamente sin intervención del usuario.
 - El usuario no puede inhabilitar ni eliminar la extensión.

```
{ "*": {"installation_mode": "force_installed" } }
```
- "normal_installed"
La extensión se instala automáticamente sin intervención del usuario, pero este puede inhabilitarla.

```
{ "*": {"installation_mode": "normal_installed" } }
```

- "removed"
(Chrome 75 o versiones posteriores) Los usuarios no pueden instalar la extensión. Si los usuarios han instalado la extensión anteriormente, el navegador Chrome la eliminará.

```
{ "*" : { "installation_mode": "removed" } }
```

- "toolbar_pin"

Permite controlar si el icono de la extensión se fija a la barra de herramientas. Puedes definir las opciones siguientes:

force_pinned: el icono de la extensión se fija a la barra de herramientas y se muestra siempre. El usuario no puede ocultarlo en el menú de extensiones.

default_unpinned: la extensión primero está oculta en el menú de extensiones y el usuario puede fijarla a la barra de herramientas.

Si no se define ningún valor en este campo, el ajuste predeterminado será default_unpinned.

```
{ "*" : { "toolbar_pin": "forced_pinned" } }
```

Si una extensión usa la función installation_mode, también se debe definir otro campo "update_url" que dirija a la ubicación desde donde se puede instalar la extensión.

- Si la extensión que vas a descargar se aloja en Chrome Web Store, usa ["https://clients2.google.com/service/update2/crx"](https://clients2.google.com/service/update2/crx).
- Si la extensión está alojada en tu propio servidor, especifica la URL de donde Chrome puede descargar la extensión empaquetada (archivo .crx).
Ejemplo de JSON con una extensión force_installed y update_url:

```
{ "nckgahadagoaajjgafhacjanaoiihapd": { "installation_mode": "force_installed", "update_url": "https://clients2.google.com/service/update2/crx" } }
```
- Desde Chrome 89, también se puede utilizar el ajuste override_update_url para especificar que Chrome use la URL del campo update_url o la URL de actualización especificada en la política ExtensionInstallForcelist para posteriores actualizaciones de la extensión.
 - Si no se define esta política o se le asigna el valor false, Chrome usará la URL especificada en el archivo de manifiesto de la extensión para las actualizaciones.

Impedir que las extensiones modifiquen páginas web

Este ajuste impide que las extensiones cambien y lean los datos de tus sitios web que contienen la información más sensible.

Esta política impedirá que las extensiones hagan lo siguiente:

- Insertar secuencias de comandos en tus sitios web.
- Leer las cookies.
- Hacer modificaciones en solicitudes web.

Este ajuste no evita que los usuarios instalen o eliminen extensiones. Solamente impide que las extensiones cambien los sitios web que especifiques.

Con esta función se pueden usar estos dos ajustes:


- **runtime_blocked_hosts:** impide que las extensiones interactúen con los hosts de esta lista.

- **runtime_allowed_hosts:** las extensiones pueden interactuar con los hosts de esta lista aunque se hayan definido en runtime_blocked_hosts.

Nota: Cada instancia de runtime_blocked_hosts y de runtime_allowed_hosts puede tener 100 patrones de host como máximo. Si defines una cantidad mayor, la política no será válida.

Gestión en la nube del navegador Chrome

Bloquear por host en tiempo de ejecución resulta más sencillo con [Gestión en la nube del navegador Chrome](#) que con GPO. No es necesario utilizar JSON y solo hay que especificar la URL que se quiera bloquear en la configuración de extensiones. Para configurarlo, tienes que registrar los dispositivos donde uses el navegador en Gestión en la nube del navegador Chrome. Esta función se ofrece sin coste adicional. Consulta los pasos para realizar el registro en [esta página](#).

1. En la consola de administración, ve a **Dispositivos > Chrome > Aplicaciones y extensiones > Usuarios y navegadores**.
2. Selecciona la unidad organizativa donde estén los usuarios para los que quieras permitir las extensiones.
3. Haz clic en el icono de la rueda dentada de Configuración adicional .
4. En la sección "Hosts bloqueados en tiempo de ejecución", escribe la URL de los sitios web con información sensible donde no quieras que se ejecuten las extensiones. Para obtener información sobre la sintaxis, revisa la [sintaxis de las URLs bloqueadas y permitidas](#).
 - a. Para especificar varias URLs, pulsa Intro después de cada URL para añadir una nueva entrada.
 - b. También puedes hacer clic en una extensión individual y definir hosts permitidos y bloqueados en la sección de acceso mediante permisos y URLs.
 - i. Ten en cuenta que este ajuste anulará cualquier política global que ya se esté aplicando a esta extensión.
 - ii. También hay una sección de allowed_hosts para las excepciones de las URLs incluidas en la sección de hosts bloqueados en tiempo de ejecución.
5. Haz clic en **Guardar**.

Hosts bloqueados en tiempo de ejecución

***://*.sensitivesite.com**

Se trata de una lista de patrones de correspondencias con nombres de hosts. Las aplicaciones y extensiones no pueden modificar las URLs que coincidan con uno de estos patrones. Por ejemplo, no pueden insertar JavaScript, ver ni modificar los elementos webRequests o webNavigation ni las cookies, ignorar la política de origen único, etc. El formato es similar al de los patrones de URLs completas, pero no se pueden definir rutas (por ejemplo, "*://*.examplecom")

Hosts permitidos en tiempo de ejecución

Hosts con los que las extensiones pueden interactuar, aunque figuren en la lista de hosts bloqueados en tiempo de ejecución. Hay que usar el mismo formato que en dicha lista.

Sección de hosts en tiempo de ejecución disponible en Dispositivos > Chrome > Aplicaciones y extensiones > Usuarios y navegadores > Configuración adicional

GPO

En estas instrucciones se explica cómo gestionar este GPO en equipos Windows. Para ver las instrucciones de otras plataformas, consulta estas referencias: [Mac](#) | [Linux](#)

Dentro de la política de configuración de extensiones, puedes definir estos ajustes para bloquear (o permitir) las modificaciones en sitios web o en dominios:

- `runtime_blocked_hosts`
Este ajuste impide que las extensiones hagan cambios o lean datos en los sitios web que elijas.
- `runtime_allowed_hosts`
Este ajuste permite que las extensiones hagan cambios o lean datos en los sitios web que elijas.

El formato para especificar los sitios en la cadena JSON de la política es el siguiente:

```
[http|https|ftp|*]://[subdomain|*].[hostname|*].[eTLD|*] [http|https|ftp|*],
```

Nota: Las secciones `[hostname|*]` y `[eTLD|*]` son obligatorias, pero `[subdomain|*]` es opcional.

Ejemplos de patrones de host válidos y de coincidencias:

Patrones de host válidos	Coincide con	No coincide con
<code>*://*.example.*</code>	<code>http://example.com</code> <code>https://test.example.co.uk</code>	<code>https://example.google.com</code> <code>http://example.google.co.uk</code>
<code>http://example.*</code>	<code>http://example.com</code> <code>http://example.ly</code>	<code>https://example.com</code> <code>http://test.example.com</code>
<code>http://example.com</code>	<code>http://example.com</code>	<code>https://example.com</code> <code>http://test.example.co.uk</code>
<code>*://*</code>	Todas las URLs	

Este es un ejemplo de una cadena JSON que bloquea el acceso a una sola extensión. La cadena evita que una extensión individual aumente un sitio concreto:

```
{  
  "aapbdbdomjkkjkaonfhkkikfgjllcleb": {  
    "runtime_blocked_hosts": ["*://*.importantwebsite"]  
  }  
}
```

Datos JSON compactos:

```
{"aapbdbdomjkkjkaonfhkkikfgjllcleb":  
{"runtime_blocked_hosts":["*://*.importantwebsite"]}}
```

Este es un ejemplo de cómo bloquear varios sitios para todas las extensiones:

```
{  
  "*": {"runtime_blocked_hosts": [ "*://*.importantwebsite.com",  
"*://*.importantwebsite2.com" ]  
}
```

Datos JSON compactos:

```
{"*":{"runtime_blocked_hosts":["*://*.importantwebsite.com","*://*.importantweb  
site2.com"]}}
```

Cuando haya varias extensiones, separa cada una en su propia entrada por cada ID de aplicación que quieras bloquear. Este es un ejemplo de cómo impedir que se ejecuten dos extensiones en el mismo dominio:

```
{  
  "aapbdbdomjkkjkaonfhkkikfgjllcleb": {  
    "runtime_blocked_hosts": ["*://*.importantwebsite"]  
  },  
  "bfbmjmiodbnnpllbbbfblcplfjjepjdn": {  
    "runtime_blocked_hosts": ["*://*.importantwebsite"]  
  }  
}
```

Datos JSON compactos:

```
{"aapbdbdomjkkjkaonfhkkikfgjllcleb": {"runtime_blocked_hosts":  
["*://*.importantwebsite"]}, "bfbmjmiodbnnpllbbbfblcplfjjepjdn":  
{"runtime_blocked_hosts": ["*://*.importantwebsite"]}}
```

Permitir o bloquear extensiones en la consola de administración de Google

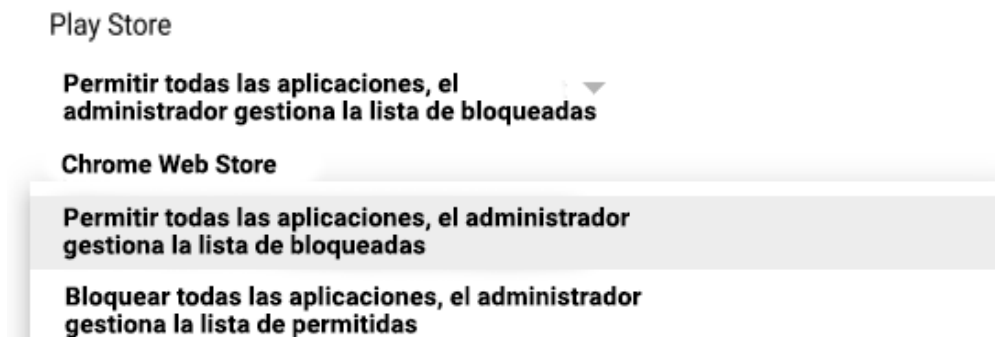
Los administradores pueden crear listas de extensiones permitidas y bloqueadas para controlar qué extensiones pueden instalar los usuarios. Puedes permitir que los usuarios instalen cualquier aplicación o extensión. También puedes definir políticas para bloquear o permitir aplicaciones en las cuentas de todos los usuarios o solo de empleados concretos.

En este procedimiento se presupone que ya sabes cómo modificar ajustes en la consola de administración.

Permitir todas las extensiones excepto las que quieras bloquear

1. En la consola de administración, ve a **Dispositivos > Chrome > Aplicaciones y extensiones > Usuarios y navegadores > Configuración adicional**.
2. En la parte izquierda, selecciona la unidad organizativa en la que quieras permitir las extensiones.
3. Desplázate hacia abajo hasta la sección Modo de permiso/bloqueo, situada debajo de Chrome Web Store, haz clic en Editar y selecciona la opción **Permitir todas las aplicaciones, el administrador gestiona la lista de bloqueadas**.

Editar el ajuste Modo de permiso/bloqueo



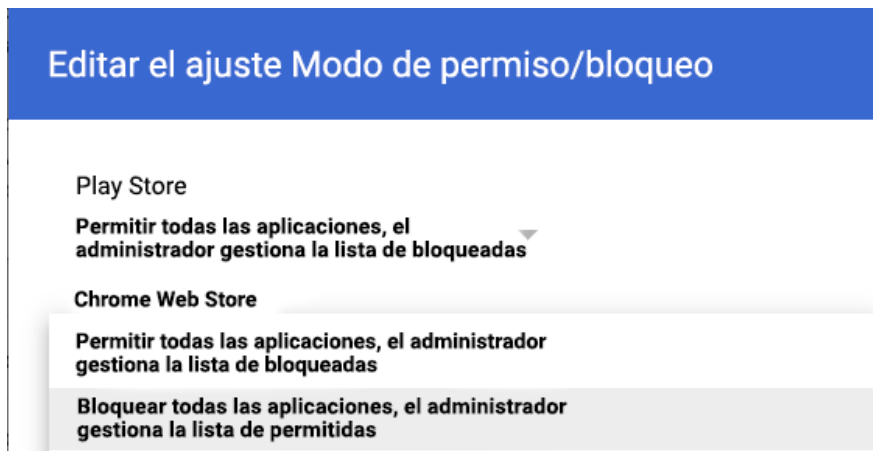
Ajuste del modo de permiso/bloqueo

4. Haz clic en **Guardar**.
5. Haz clic en la pestaña Usuarios y navegadores para volver a la página anterior.
6. Para añadir cada extensión que quieras bloquear, haz clic en el signo más de color amarillo situado abajo a la derecha.
7. Elige el método que quieres usar para añadirlas a la consola (desde Chrome Web Store, por ID de extensión o por URL).
8. Selecciona el menú desplegable situado junto a la extensión y elige **Bloquear**.

9. Haz clic en **Guardar**.

Bloquear todas las extensiones excepto las que quieras permitir

1. En la consola de administración, ve a **Dispositivos > Chrome > Aplicaciones y extensiones > Usuarios y navegadores > Configuración adicional**.
2. En la parte izquierda, selecciona la unidad organizativa en la que quieras bloquear las extensiones.
3. Desplázate hacia abajo hasta la sección Modo de permiso/bloqueo, situada debajo de Chrome Web Store, y selecciona la opción **Bloquear todas las aplicaciones, el administrador gestiona la lista de permitidas**.

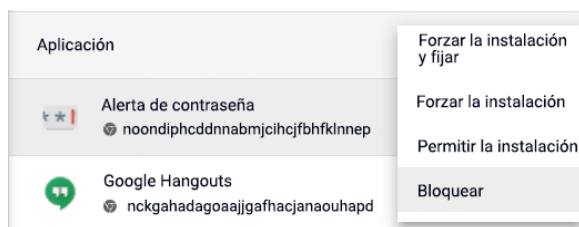


4. Haz clic en **Guardar**.
5. Haz clic en la pestaña Usuarios y navegadores para volver a la página anterior.
6. Para añadir cada extensión que quieras permitir, haz clic en el signo más de color amarillo situado abajo a la derecha.
7. Elige el método que quieres usar para añadirlas a la consola (desde Chrome Web Store, por ID de extensión o por URL).
8. Selecciona el menú desplegable situado junto a la extensión y elige **Permitir la instalación**.
 - a. También puedes forzar la instalación de la extensión en los equipos de los usuarios seleccionando Forzar la instalación.
9. Haz clic en **Guardar**.

Bloquear o permitir una extensión

1. En la consola de administración, ve a **Dispositivos > Chrome > Aplicaciones y extensiones > Usuarios y navegadores**.
2. Selecciona la unidad organizativa en la que quieras permitir o bloquear la extensión.
 - o Nota: Aunque la unidad organizativa heredará los ajustes de la unidad organizativa superior, puedes anularlos en una unidad organizativa secundaria concreta.
3. Selecciona la extensión que quieras bloquear, permitir o añadir (consulta los pasos 6 y 7 del apartado anterior).

4. En la columna de la política de instalación, selecciona la opción correspondiente para bloquear,



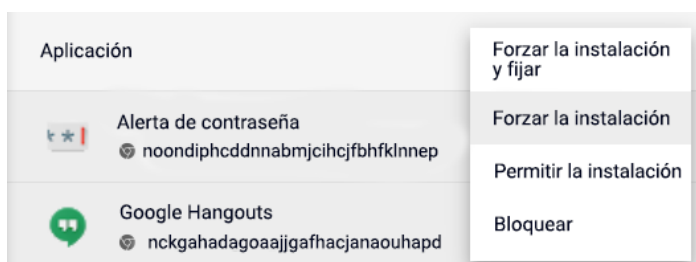
forzar la instalación o permitir la instalación.

5. Haz clic en **Guardar**.

Instalación forzada de extensiones

Si sabes que un usuario necesita una extensión, puedes forzar su instalación. En este caso, se concederán a la extensión todos los permisos que necesita para ejecutarse. Además, el usuario no podrá eliminarla y la instalación se hará de forma silenciosa. Si eliminas una extensión de la lista de instalación forzada, se eliminará del equipo del usuario.

1. En la consola de administración, ve a **Dispositivos > Chrome > Aplicaciones y extensiones > Usuarios y navegadores**.
2. Selecciona la unidad organizativa en la que quieras forzar la instalación de extensiones.
3. Selecciona las extensiones que quieras instalar de manera forzada o añádelas si todavía no las tienes.
 - a. Para añadir las extensiones que quieras instalar, haz clic en el signo más de color amarillo situado abajo a la derecha.
 - b. Elige el método que quieres usar para añadirlas a la consola (desde Chrome Web Store, por ID de extensión o por URL).
4. Selecciona las extensiones de instalación forzada y, en la columna de la política de instalación, selecciona la opción **Forzar la instalación** del menú desplegable.



5. Haz clic en **Guardar**.

Ten en cuenta que puedes crear una colección personalizada de Chrome Web Store con las extensiones seleccionadas por el administrador que se mostrarán a los usuarios. Este ajuste no requiere que los usuarios hayan iniciado sesión con sus identidades de Google utilizando credenciales de empresa.

- Para acceder a este ajuste en la consola de administración, ve a Dispositivos > Chrome > Aplicaciones y extensiones > Usuarios y navegadores > Configuración adicional > Página principal de Chrome Web Store > Utilizar colección de Chrome Web Store.
 - Luego, puedes hacer que todas las extensiones se muestren en esa página o puedes elegir extensiones concretas en la sección Usuarios y navegadores, y seleccionar la opción Incluir en la colección de Chrome Web Store.

Permitir que los usuarios soliciten extensiones: flujos de trabajo de extensiones

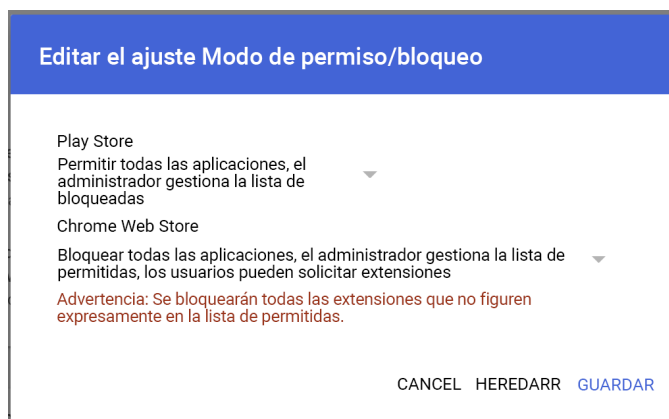
Como administrador, puedes utilizar la consola de administración de Google para permitir que los usuarios soliciten las extensiones de Chrome Web Store que necesiten. Después, podrás permitir, bloquear o instalar automáticamente las extensiones que hayan solicitado los usuarios.



Ejemplo del cuadro de diálogo de solicitud de Chrome Web Store

Ten en cuenta que esta función actúa como una lista de permitidos o bloqueados. Cuando está activada, se bloquean **todas** las extensiones de forma predeterminada. Para evitar problemas, te recomendamos que sigas este procedimiento:

1. Averigua qué extensiones utilizan actualmente tus usuarios con el [informe de exportación de extensiones](#) de Gestión en la nube del navegador Chrome.
 - Para obtener más información, consulta este [vídeo de YouTube sobre cómo configurar la API de Takeout](#).
2. Crea una lista de extensiones esenciales (mediante [GPO](#) o la [consola de administración](#)) basándote en los datos recogidos en el primer paso.
3. Activa la función de flujo de trabajo de extensiones en **Dispositivos > Chrome > Aplicaciones y extensiones > Usuarios y navegadores > Configuración adicional** > Modo de permiso/bloqueo y haz clic en el botón Editar.
4. En Chrome Web Store, selecciona **Bloquear todas las aplicaciones, el administrador gestiona la lista de permitidas, los usuarios pueden solicitar extensiones** en el menú desplegable.



Habilitar flujos de trabajo de extensiones en la consola de administración

- Te recomendamos que primero apliques los ajustes a un número reducido de usuarios y de dispositivos en una unidad organizativa de prueba para evitar problemas a los usuarios finales y recabar opiniones. Cuando esté todo listo, puedes aplicar la configuración a toda la organización.
5. Las solicitudes de aprobación y denegación se gestionan en **Dispositivos > Chrome > Aplicaciones y extensiones > Solicitudes**.
 6. Haz clic en la fila de la solicitud de extensión que quieras revisar.
 7. Aquí puedes consultar detalles sobre la extensión y seleccionar la política de instalación en el menú desplegable:
 - Forzar la instalación: instala la extensión de manera silenciosa e impide que se elimine.
 - Permitir la instalación: permite que los usuarios instalen la extensión.
 - Bloquear: impide que los usuarios instalen la extensión. También elimina la extensión de los equipos de los usuarios que la tengan instalada.

Para obtener más información acerca de esta función, consulta el [artículo del Centro de Ayuda sobre flujos de trabajo de extensiones](#) o este [vídeo de YouTube sobre el mismo tema](#).

Permitir o bloquear extensiones en Directiva de grupo

Antes de empezar: En este procedimiento se presupone que ya gestionas Chrome en las cuentas de tus usuarios. Si quieres ver más información sobre cómo implementar Chrome en Windows, consulta la [Guía de implementación del navegador Chrome \(Windows\)](#). Para obtener información sobre la implementación y la gestión de políticas en Mac®, consulta el artículo [Configurar el navegador Chrome en Mac](#).

Para Windows, hay dos tipos de plantillas de políticas: ADM y ADMX. Verifica qué tipo puedes utilizar en tu red. Las plantillas indican las claves de registro que puedes definir para configurar Chrome, así como sus posibles valores. Los valores definidos en estas claves de registro determinan el comportamiento de Chrome.

1. Descarga las plantillas de políticas de Chrome.
Puedes obtener las plantillas de Windows y la documentación sobre las plantillas de políticas comunes a todos los sistemas operativos en [este enlace](#).

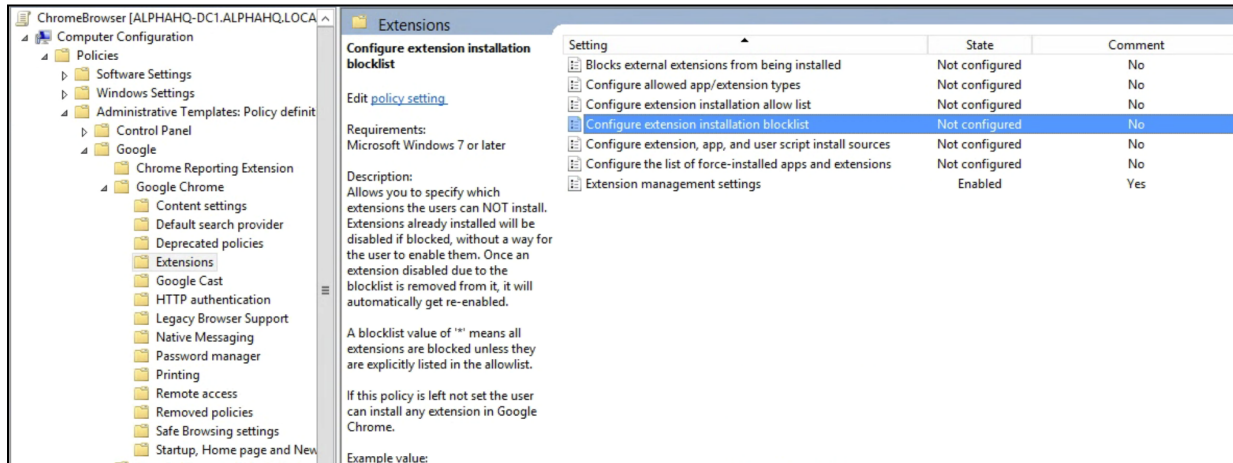
2. Para abrir la plantilla ADM o ADMX que has descargado, sigue estos pasos:
 - a. Ve a **Inicio > Ejecutar: gpedit.msc**.
 - b. Accede a **Directiva de equipo local > Configuración del equipo > Plantillas administrativas**.
 - c. Haz clic con el botón derecho en **Plantillas administrativas** y selecciona **Agregar o quitar plantillas**.
 - d. Añade la plantilla chrome.adm mediante el cuadro de diálogo.

Una vez hecho esto, aparecerá una carpeta llamada Google o Google Chrome en Plantillas administrativas (si no estaba anteriormente).

- Si has añadido la plantilla ADM en Windows 7 o 10, aparecerá en Plantillas administrativas clásicas (ADM) > Google > Google Chrome.

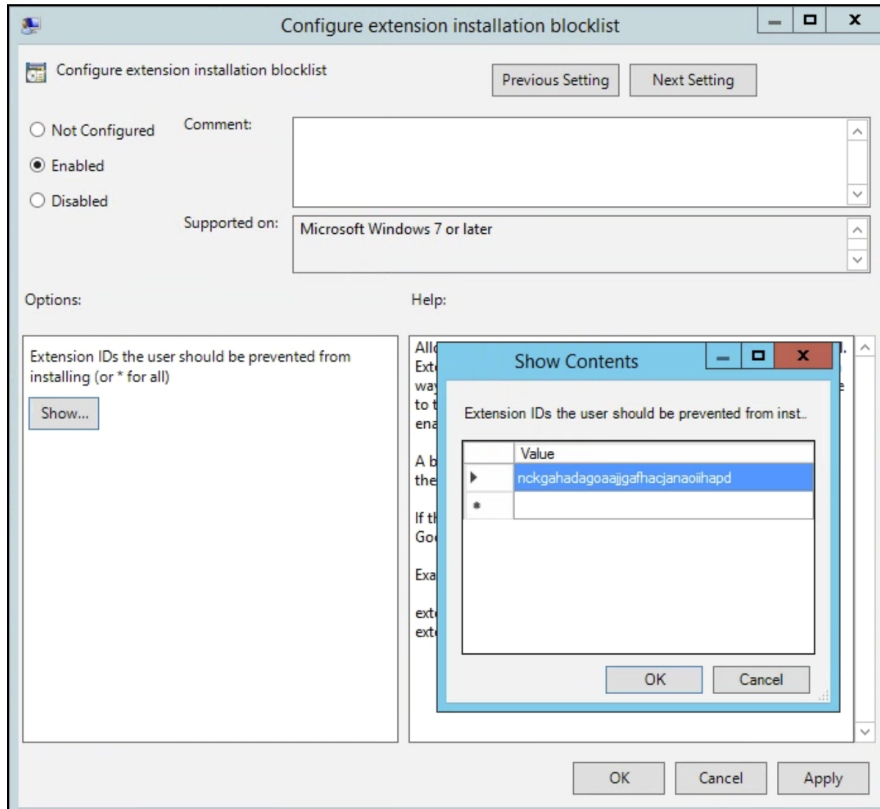
Permitir todas las extensiones excepto las que quieras bloquear

1. En el editor de directivas de grupo, abre la plantilla que acabas de añadir.
2. Ve a **Google > Google Chrome > Extensiones > Configurar lista de bloqueados de instalación de extensiones**.



Ruta a las políticas de gestión de extensiones

2. En el ajuste, selecciona **Habilitada**.
3. Haz clic en **Mostrar**.
4. Escribe el ID de aplicación de las extensiones que quieras bloquear.



Configurar lista de bloqueados de instalación de extensiones

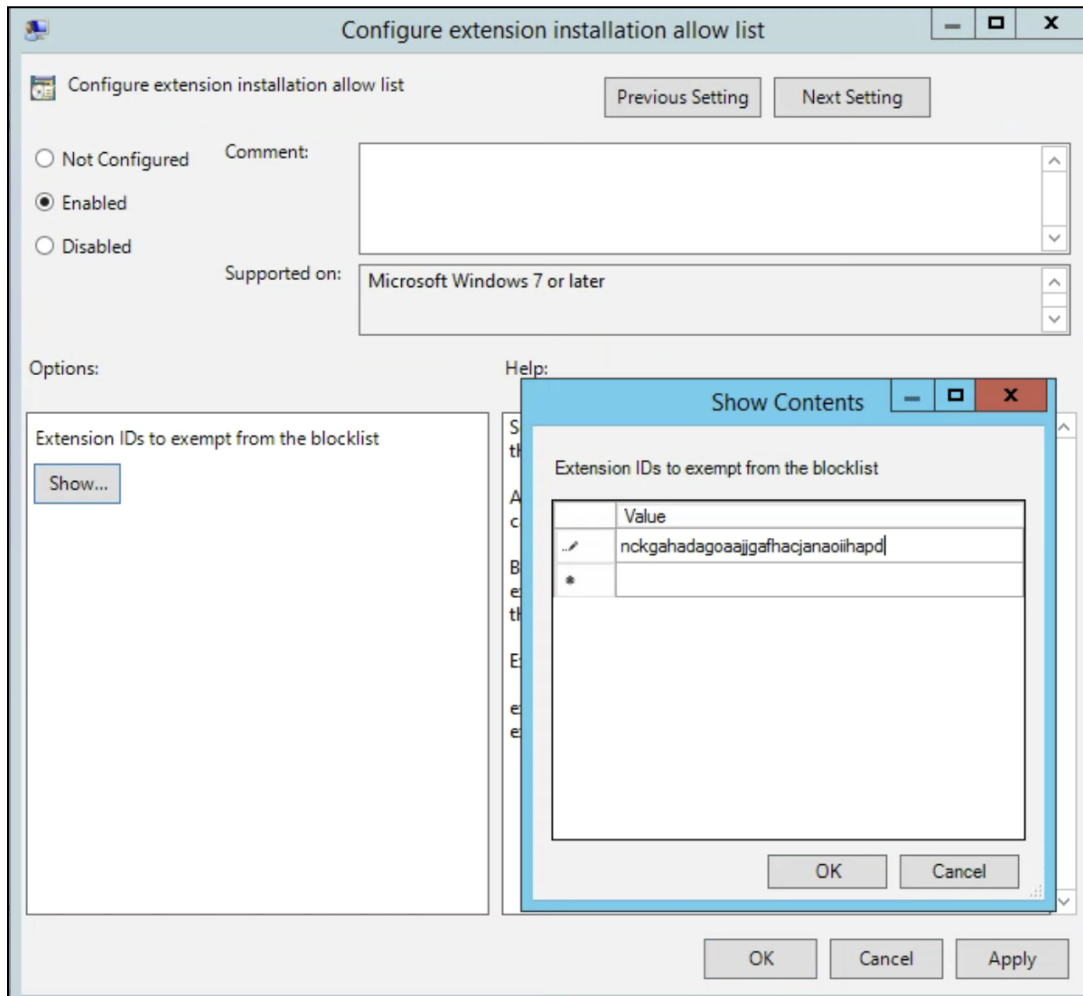
Notas:

- Si no encuentras el ID de aplicación de una extensión, consúltalo en Chrome Web Store. Busca la extensión concreta y verás el ID de aplicación al final de la URL en el omnibox de Chrome:

https://chrome.google.com/webstore/detail/google-hangouts/nckgahadagoaajjgafhacjanaoiihapd

Ejemplo de ID de aplicación que se muestra detrás de google-hangouts/

- Escribe * en la política para evitar que se instale cualquier extensión. Puedes seguir este procedimiento con la política Configura la lista de extensiones de instalación permitidas. De este modo, solo permitirás que los usuarios instalen determinadas extensiones y bloquearás el resto.
- Puedes añadir a la lista de bloqueadas una extensión que ya esté instalada en el equipo de un usuario. Al hacerlo, la extensión se inhabilitará y se impedirá que el usuario la vuelva a habilitar. No se desinstalará; solo se inhabilitará.



Configura la lista de extensiones de instalación permitidas

Bloquear o permitir una extensión

Para bloquear solo una extensión, añade el ID de aplicación de la extensión que quieras bloquear a la política Configurar lista de bloqueados de instalación de extensiones. Todas las demás extensiones se podrán instalar.

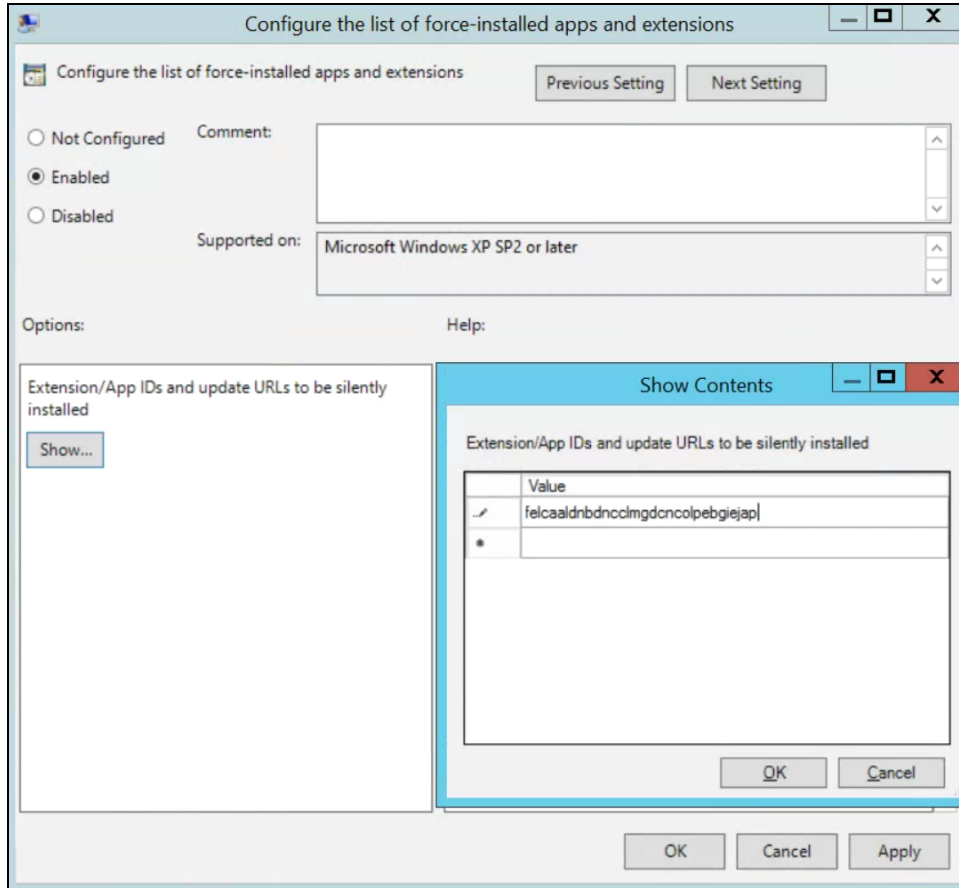
Para permitir solo una extensión:

1. En la sección de contenido de la política Configurar lista de bloqueados de instalación de extensiones, escribe *.
De este modo impedirás que se instale cualquier extensión que esté en la lista.
2. Añade el ID de aplicación de la extensión permitida a la política Configurar lista de bloqueados de instalación de extensiones.

Forzar la instalación de una extensión

1. En el editor de directivas de grupo, ve a **Google > Google Chrome > Extensiones > Configura la lista de aplicaciones y extensiones de instalación forzada**.
2. Selecciona **Habilitada**.
3. Haz clic en **Mostrar**.
4. Escribe los IDs de aplicación de las extensiones que quieras instalar de manera forzada.

Las extensiones se instalarán de forma silenciosa y sin intervención del usuario. Además, el usuario no podrá desinstalarlas ni inhabilitarlas. Este ajuste anulará cualquier política de lista de bloqueados que se pueda haber habilitado.



Configura la lista de aplicaciones y extensiones de instalación forzada

Validar la política

Para asegurarte de que la política que has definido es válida y funciona del modo esperado, aplícala a un equipo de prueba. En el equipo de prueba, sigue los pasos que se indican a continuación.

1. Ve a `chrome://policy`.
2. Haz clic en el botón "Volver a cargar políticas".
3. En la esquina superior derecha de la página está el filtro de políticas. Escribe "ExtensionSettings" para mostrar solo esta política.
4. Marca la casilla "Mostrar políticas sin valores establecidos".
5. Comprueba que en la columna "Estado" de tu política se muestre "OK".
6. Haz clic en "Mostrar valor" para expandir la política y asegúrate de que el campo no esté vacío.
7. ¡Enhorabuena! Ya tienes una política válida.

Alojar tus extensiones en servidores propios

[Chrome Web Store](#) aloja extensiones y ofrece numerosas funciones de seguridad.

- Funciones como análisis automáticos y manuales del código.
 - De este modo se impide que se envíe código malicioso a los usuarios.

Sin embargo, existe la posibilidad de alojar las extensiones en un servidor propio e independiente de Chrome Web Store. Este método presenta algunas ventajas e inconvenientes:

Ventajas:

- Alojamiento de tus propias extensiones significa que no están sujetas a las reglas y los requisitos de Chrome Web Store.
 - Por lo tanto, las extensiones no están sometidas a tanto escrutinio y hay menos riesgo de que se puedan eliminar por infringir los términos del servicio.

Inconvenientes:

- El método de alojamiento en servidores propios requiere más configuración y obliga a tener un servidor de archivos propio para los archivos de extensiones.
- Validar la seguridad de las extensiones y mantenerlas actualizadas puede ser una tarea ardua, mientras que Chrome Web Store lo hace automáticamente.

Si te decantas por alojar las extensiones en servidores propios, en este apartado se indica cómo hacerlo. En él encontrarás información sobre cómo empaquetar una extensión y cómo alojarla sin usar Chrome Web Store. También proporciona instrucciones para implementar las extensiones en tus dispositivos y cuentas de usuario.

Alternativas a alojar las extensiones en servidores propios

Opciones de publicación de extensiones

Como alternativa al alojamiento en servidores propios, puedes plantearte marcar como privadas las extensiones internas que hay en Chrome Web Store. Las extensiones se pueden publicar de tres formas: pública, privada y sin mostrar. Consulta este gráfico para ver las ventajas e inconvenientes de cada una de ellas:

	¿Aparece en la búsqueda de Chrome Web Store?	¿Requiere iniciar sesión?	¿Es compatible con Gestión en la nube del navegador Chrome?
Pública	Sí	No	Sí
Privada	No	Sí	Sí
Sin mostrar	No	No, los usuarios necesitan un enlace para instalarla	Sí

Para obtener más información, consulta [esta entrada de blog](#) sobre cómo publicar tus extensiones de modo privado, sin necesidad de alojarlas en servidores propios.


- Ten en cuenta que si gestionas tus extensiones mediante la consola de administración, tienes que configurar los ajustes de permisos de Chrome Web Store para permitir que las extensiones privadas se muestren a tus usuarios.

- Para acceder a este ajuste en la consola de administración, ve a Dispositivos > Chrome > Aplicaciones y extensiones > Configuración adicional > Permisos de Chrome Web Store y selecciona la opción Permitir que los usuarios publiquen aplicaciones privadas restringidas a tu dominio en Chrome Web Store.

Fijar una versión concreta de una extensión en la consola de administración

La consola de administración de Google ahora ofrece algunas opciones nuevas para la gestión de extensiones. La primera es la posibilidad de fijar una versión de una extensión directamente en la consola de administración. Esta opción ofrece mayor estabilidad a las empresas que necesitan conservar una determinada versión de una extensión. No se recomienda fijar versiones anteriores de las extensiones. En caso de hacerlo, debería ser una medida temporal hasta comprobar que se tienen las funciones y actualizaciones de seguridad más recientes. Esta función solo está disponible para las extensiones de instalación forzada. [Para obtener más información, consulta esta entrada del Centro de Ayuda.](#)

1. En la consola de administración, ve a **Dispositivos > Chrome > Aplicaciones y extensiones > Usuarios y navegadores**.
2. Selecciona la unidad organizativa que contenga la extensión que quieras fijar.
3. Selecciona las extensiones que quieras gestionar por versión o añádelas si todavía no las tienes. A continuación, debajo de la columna Versiones fijas, en el menú desplegable, selecciona la versión que quieras fijar y haz clic en Guardar.
 - a. Ten en cuenta que, al fijar una aplicación o extensión, esta ya no recibirá ninguna actualización, incluidas actualizaciones de seguridad y compatibilidad.
 - b. También puedes fijar exclusivamente la versión actual de la extensión que haya en Chrome Web Store en el momento de la configuración.
 - c. Asimismo, puedes fijar aplicaciones y extensiones alojadas en servidores propios y actualizar la URL desde la consola de administración. Consulta la sección [Fijar aplicaciones alojadas en servidores propios en este artículo del Centro de Ayuda.](#)

Descripción general	Usuarios y navegadores	Kiosco
Play Store Permitir todas las aplicaciones, el administrador gestiona la lista de bloqueadas + Haz una búsqueda o añade un filtro	Chrome Web Store Permitir todas las aplicaciones, el administrador gestiona la lista de bloqueadas	
App	Política de instalación	Versiones fijas
 Earth View from Google Earth bhloflhklmhfpedakmangadcdofhnoh	Forzar la instalación Se ha añadido de forma local	Sin fijar 3.0.5 (más reciente) <small>predeterminado</small>

Versiones fijas en la consola de administración

Requisitos para alojar extensiones en servidores propios

Para alojar tus extensiones, necesitas tus propios servicios de alojamiento web para la extensión y su archivo de manifiesto. Esa ubicación de alojamiento no debería requerir autenticación. Deberá estar

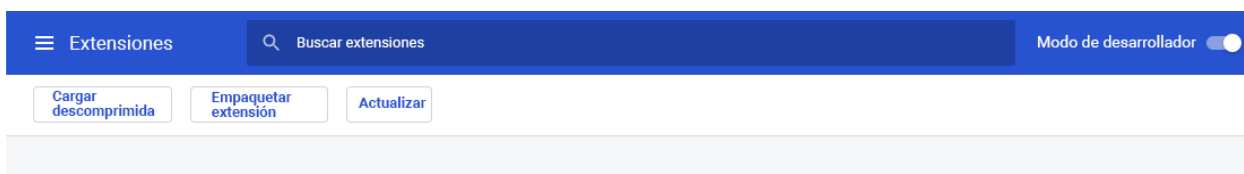
accesible para los dispositivos desde cualquier ubicación donde se utilicen. Ten esto en cuenta si quieres alojar el archivo en tu repositorio interno.

En este procedimiento se presupone que ya has creado la extensión y que tienes experiencia con los archivos XML. También, que conoces las directivas de grupo y que sabes cómo usar el registro de Windows. Estos pasos no se aplican a extensiones de terceros que no hayas desarrollado. Si quieres alojar una extensión de terceros en tus propios servidores, deberías tratar esta cuestión directamente con el proveedor de la extensión.

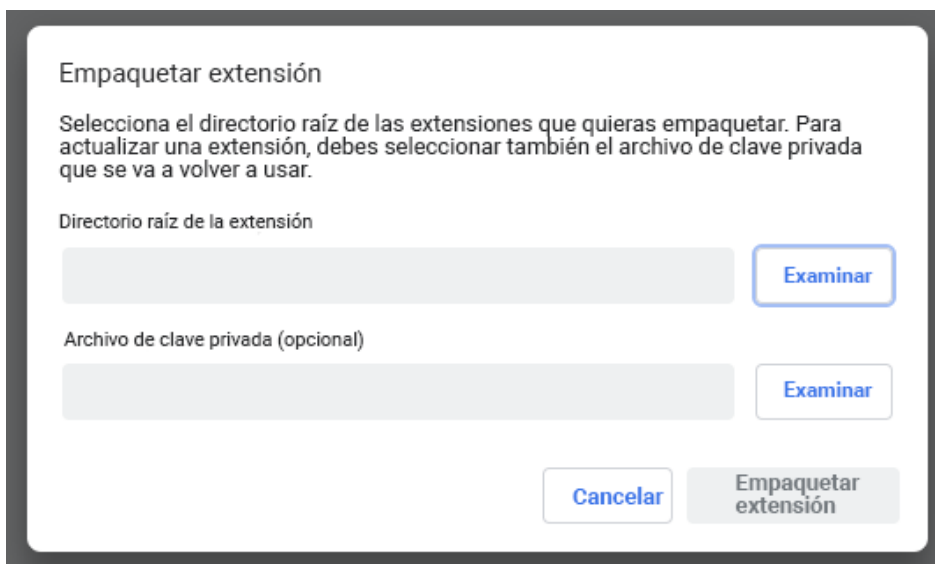
Empaquetar la extensión

Las extensiones primero se deben empaquetar en un archivo CRX. Si la extensión no está empaquetada como archivo CRX, sigue estos pasos:

1. Escribe **chrome://extensions** en la barra de direcciones de Chrome y marca la casilla **Modo de desarrollador**.

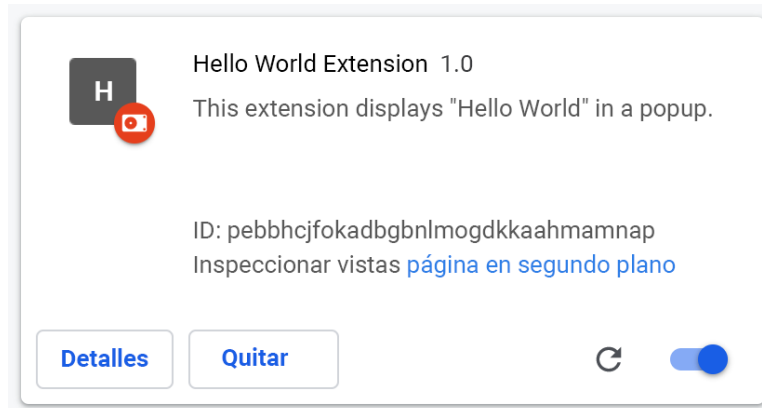


2. Una vez que estés en el modo desarrollador, crea el archivo CRX haciendo clic en **Empaquetar extensión**.



3. Selecciona el directorio donde esté tu fuente. Se creará el archivo CRX y también un archivo PEM. **Consejo:** Guarda el archivo PEM en una ubicación segura porque es la clave de tu extensión. Tendrás que utilizarlo en futuras actualizaciones.

4. Arrastra el archivo CRX a la ventana de extensiones y asegúrate de que se carga.
 - a. Ten en cuenta que la extensión estará inhabilitada de forma predeterminada en Windows y en Mac, pero no en Linux.
5. Prueba la extensión y anota el campo de ID y el número de versión.
Necesitarás estos datos más adelante.



5. Coloca el archivo CRX en la ubicación del host de donde lo descargarán tus usuarios o dispositivos.
 - o Toma nota de la URL a la que has subido el archivo.
 - o Necesitarás la URL para el archivo XML de manifiesto.
6. Para crear un archivo XML de manifiesto con el ID de la aplicación o la extensión, la URL de descarga y la versión, define estos tres campos:
 - **appid** (el ID de extensión del paso 5)
 - **codebase** (la ubicación de descarga del archivo CRX del paso 3)
 - **version** (la versión de la aplicación o la extensión, que debe coincidir con la del paso 5)

Ejemplo de archivo XML de manifiesto:

```
<?xml version='1.0' encoding='UTF-8'?>
<gupdate xmlns='http://www.google.com/update2/response' protocol='2.0'>
  <app appid='abcdefghijklmnopqrstuvwxyz123456
  '>
    <updatecheck codebase='https://example.com/chrome/helloworld.crx'
    version='1.0' />
  </app>
</gupdate>
```

8. Sube el archivo XML completado a una ubicación de donde lo puedan descargar tus usuarios o dispositivos y anota la URL.

Alojar la extensión

El servidor que aloje los archivos .crx de tu extensión debe tener encabezados HTTP apropiados para permitir que los usuarios la instalen haciendo clic en un enlace.

Google Chrome considera que un archivo es instalable si se da cualquiera de las siguientes circunstancias:

- El tipo de contenido del archivo es application/x-chrome-extension
- El sufijo del archivo es .crx y se cumplen estas dos condiciones:
 - El archivo no se ofrece con el encabezado HTTP X-Content-Type-Options: nosniff
 - El archivo se ofrece con uno de los siguientes tipos de contenido:
 - cadena vacía
 - "text/plain"
 - "application/octet-stream"
 - "unknown/unknown"
 - "application/unknown"
 - "*/*"

La causa más común de que no se reconozca un archivo como instalable es que el servidor envíe el encabezado X-Content-Type-Options: nosniff. La segunda causa más habitual es que el servidor envíe un tipo de contenido desconocido, es decir, uno no incluido en la lista anterior. Para solucionar un problema de encabezado HTTP, puedes cambiar la configuración del servidor o puedes probar a alojar el archivo .crx en otro servidor.

Publicar actualizaciones para la extensión

Asegúrate de haber realizado los cambios necesarios en la extensión y de haberla probado. Para publicar actualizaciones:

1. Aumenta el número de versión de la extensión en su archivo JSON de manifiesto.
Ejemplo:
`"version": "versionString"`
Si tienes `"version": "1.0"`, puedes actualizar a `"version": "1.1"` o cualquier número superior a "1.0".
2. Actualiza `"version"` de `<updatecheck>` en el archivo XML para que coincida con el número que has utilizado en el archivo de manifiesto en el paso anterior.
Otro ejemplo:
`<updatecheck codebase='https://app.somecompany.com/chrome/helloworld.crx' version='1.1' />`
3. Vuelve a crear un archivo CRX que incluya los nuevos cambios:
 - a. Ve a **chrome://extensions** en la barra de direcciones de Chrome.
 - b. Marca la casilla **Modo de desarrollador**.
4. Para crear el archivo CRX, haz clic en **Empaquetar extensión** y selecciona el directorio donde esté tu fuente.

Nota: En el caso del archivo PEM, tienes que utilizar el mismo archivo que se generó y se guardó la primera vez que se creó el archivo CRX.

5. Arrastra el archivo CRX a la ventana de extensiones y asegúrate de que se carga.
6. Prueba la extensión.
7. Reemplaza los archivos CRX y XML anteriores por el nuevo.
 - a. Tienes que utilizar la misma ubicación de host de donde los usuarios o los dispositivos han descargado los archivos anteriormente.

Los cambios se tendrán en cuenta durante el próximo ciclo de sincronización de políticas.

URLs de referencia:

- [Actualización automática](#)
- [URL de actualización](#)
- [Archivo de manifiesto de actualización](#)

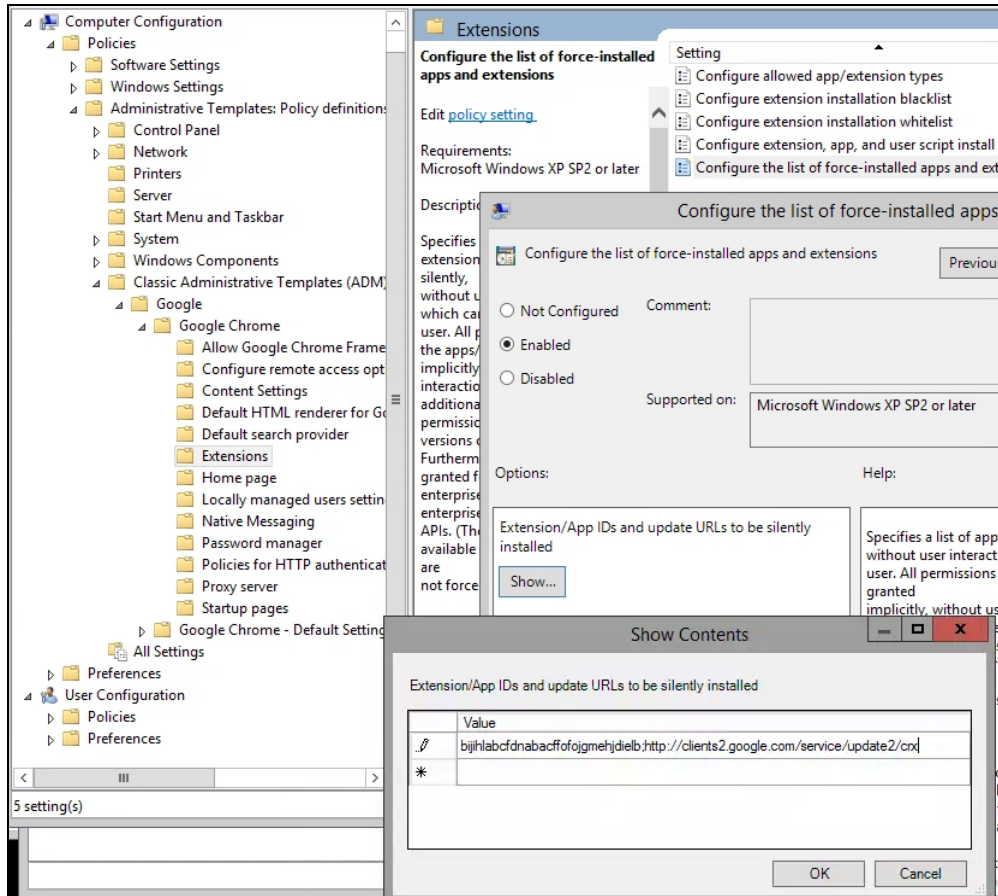
Distribuir extensiones alojadas en servidores privados

En Directiva de grupo: actualmente, solo se permite distribuir extensiones alojadas en servidores propios a través de una directiva de grupo. Puedes usar la política llamada "Configura la lista de aplicaciones y extensiones de instalación forzada" para forzar la instalación de una extensión en el dispositivo de un usuario.

En el caso de las aplicaciones alojadas en servidores privados (no en Chrome Web Store), utiliza una cadena como esta:

```
pckdojakecnnhhplcgfflhndiffaohfah;https://sites.google.com/site/pushcrx/privatewebstore/extension_info.xml
```

La URL se especifica en el archivo **update.xml de la aplicación interna**, en vez de en la URL `clients2.google.com` que se mostrará de forma pública.



Política de GPO "Configura la lista de aplicaciones y extensiones de instalación forzada" (Mostrar contenido)

Después, las políticas se pueden aplicar a usuarios y equipos seleccionados. La política puede tardar algún tiempo en aplicarse. Puedes acelerar el proceso ejecutando "gpupdate" en el equipo del usuario.

Gestionar extensiones con Gestión en la nube del navegador Chrome

Gestiona el navegador Chrome en tus equipos Windows, Mac y Linux desde un mismo lugar y accede a información detallada del estado de Chrome en tu entorno. Gestión en la nube del navegador Chrome permite gestionar fácilmente los ajustes del navegador Chrome. Puedes acceder a esta consola sin ningún coste adicional. Todas las secciones de este documento que hacen referencia a la consola de administración de Google están disponibles con esta función de Chrome. La consola te permite ver rápidamente información valiosa sobre los siguientes aspectos:

- Las versiones del navegador Chrome implementadas actualmente en tus dispositivos
- Las extensiones instaladas en cada navegador
- Las políticas que se aplican a cada navegador
- Para ver más información sobre cómo gestionar extensiones con Gestión en la nube del navegador Chrome, consulta [este vídeo](#)

Recursos adicionales

Aquí tienes más recursos que te ayudarán a gestionar el navegador Chrome en tu organización:

- [Página de Gestión en la nube del navegador Chrome](#)
- [Paquete Chrome Enterprise](#)
- [Lista de políticas de Chrome](#)
- [Notas de la versión de Chrome Enterprise](#)
- [Estrategias para la gestión de las actualizaciones de Chrome](#)
- [Centro de Ayuda de Chrome Enterprise](#)
- [Definir Chrome como navegador predeterminado \(Windows 10\)](#)
- [Serie de entradas de blog Chrome Insider](#)
- [Transición de las extensiones de Chrome a Manifest V3](#)