



Auditoría Sistema Operativo Android

Chiletti Emanuel



Herramienta


Se utilizaron recomendaciones del CIS
Benchmarks según dicta el documento CIS
Google Android benchmark en su versión 1.3.0
09-03-2019

Este documento, Security Configuration Benchmark para Google Android, proporciona una guía prescriptiva para establecer una postura de configuración segura para el sistema operativo Google Android.

Esta guía se probó con el sistema operativo Android 10.0.0. Este punto de referencia cubre Android 10.0.xy todos los dispositivos de hardware en los que se admite este sistema operativo.

Entidad auditable

Se utilizó un teléfono que contiene el sistema operativo android.



Nombre del dispositivo
Redmi Note 8

Versión MIUI
MIUI Global
12.0.5
Estable

Almacenamiento

Ocupado
23.8 GB/64 GB

Versión MIUI
MIUI Global 12.0.5
Estable
12.0.5.0(QCOMIXM)

Versión de Android
10 QKQ1.200114.002

Nivel de parche de seguridad de Android
2021-04-01



01

Configuración de seguridad

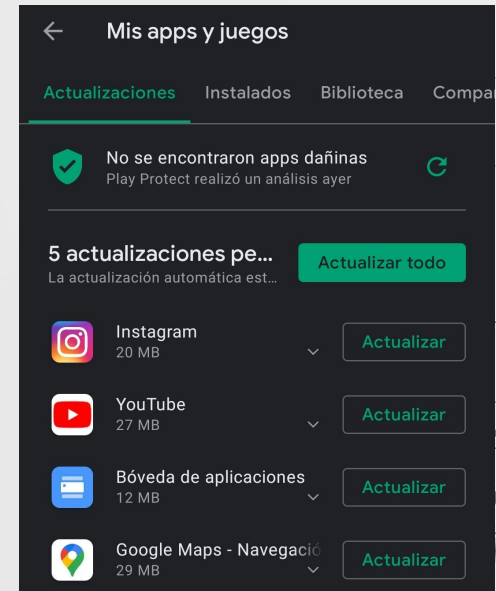
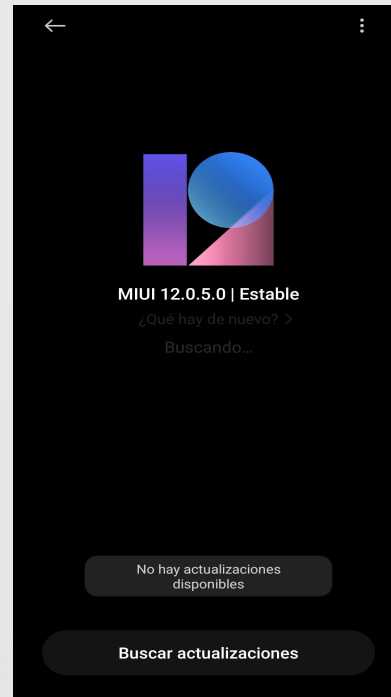
1.1 Asegúrese de que el firmware del dispositivo esté actualizado y mantener las aplicaciones del dispositivo actualizadas.

Pasos para verificar sistema:

- Ajustes
- Acerca del teléfono
- Version de MIUI
- Buscar actualizaciones

Pasos para verificar aplicaciones:

- Play Store
- Mis apps y juegos
- Actualizar todo

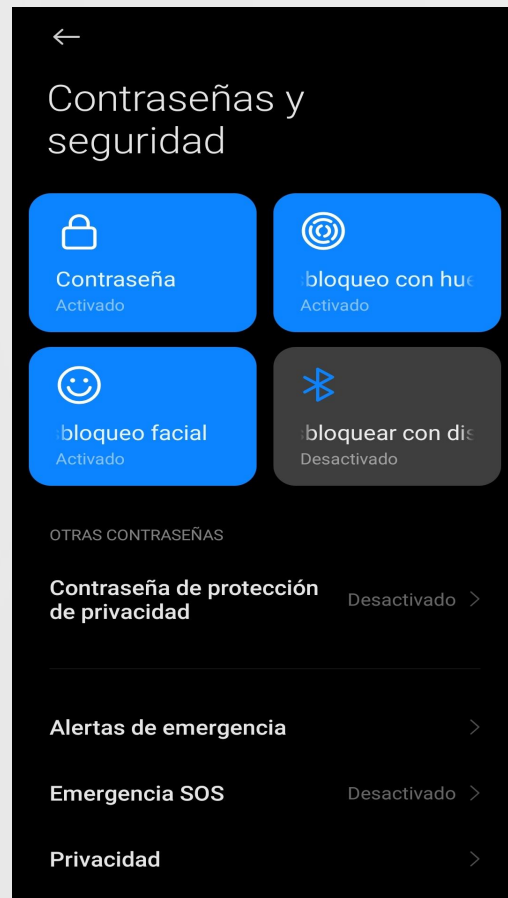


1.2 Asegúrese de que 'Bloqueo de pantalla' esté configurado en 'Habilitado'

Habilitar Bloqueo de pantalla requiere una forma de autenticación de usuario antes de interactuar con el dispositivo. Esto refuerza la protección de aplicaciones y datos y, en general, mejora la seguridad del dispositivo.

Pasos:

- Ajustes
- Contraseñas y seguridad

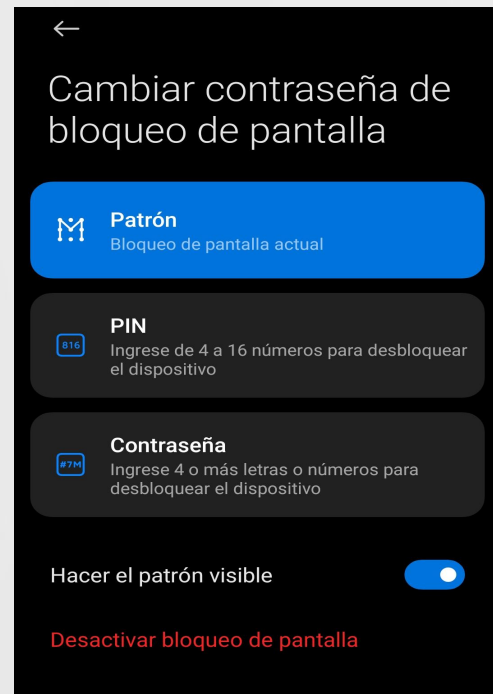


1.3 Asegúrese de que 'Hacer visible el patrón' esté configurado en 'Deshabilitado'

Mantener el patrón de desbloqueo del dispositivo visible durante el desbloqueo del dispositivo puede revelar el patrón y es vulnerable.

Pasos:

- Ajustes
- Contraseñas y seguridad
- Contraseña
- Desactivar "Hacer el patrón visible"



1.4 Asegúrese de que 'Mostrar contraseñas' esté configurado como 'Desactivado'

Esta configuración controla si las contraseñas escritas en su dispositivo Android deben estar visibles en la pantalla u ocultas al reemplazar las letras con puntos.

Pasos:

- Ajustes
- Contraseñas y seguridad
- Privacidad
- Desactivar “Mostrar Contraseñas”

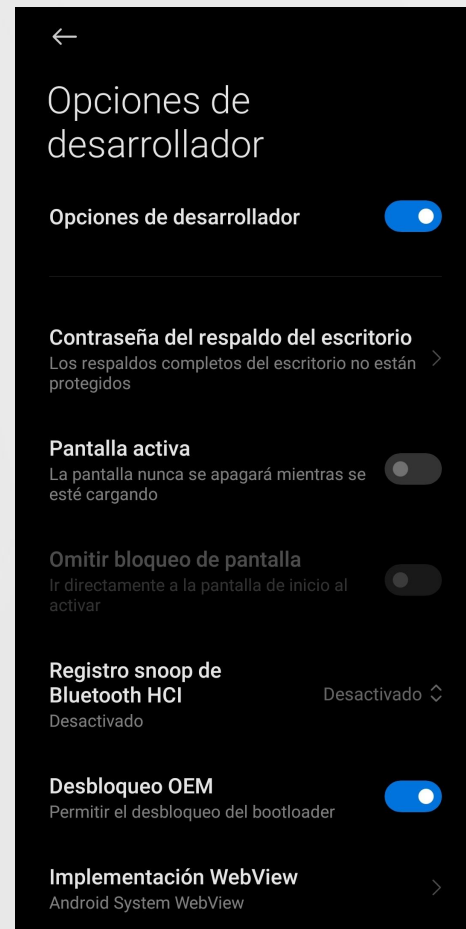


1.5 Asegúrese de que 'Opciones de desarrollador' esté configurado como 'Deshabilitado'

Habilitar Opciones de desarrollador permite a un usuario alterar drásticamente ciertas configuraciones muy avanzadas en el dispositivo. Esto puede afectar gravemente la forma en que funciona el dispositivo y expone al usuario características mayores y de desarrollo.

Pasos:

- Ajustes
- Ajustes adicionales
- Opciones de desarrollador
- Desactivar "Opciones de desarrollador"

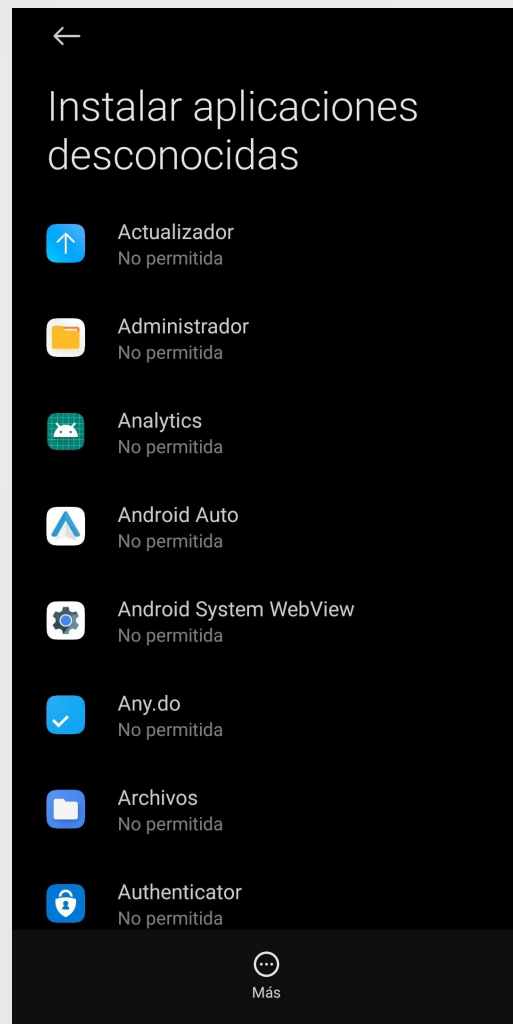


1.6 Asegúrese de que 'Instalar aplicaciones desconocidas' esté configurado como 'Deshabilitado'

Esta configuración determina si las aplicaciones se pueden instalar desde ubicaciones que no sean Google Play. La desactivación de la instalación de canales de distribución que no son de confianza protege contra la instalación accidental de aplicaciones maliciosas o que no son de confianza.

Pasos:

- Ajustes
- Protección de privacidad
- Permisos especiales
- Instalar aplicaciones desconocidas

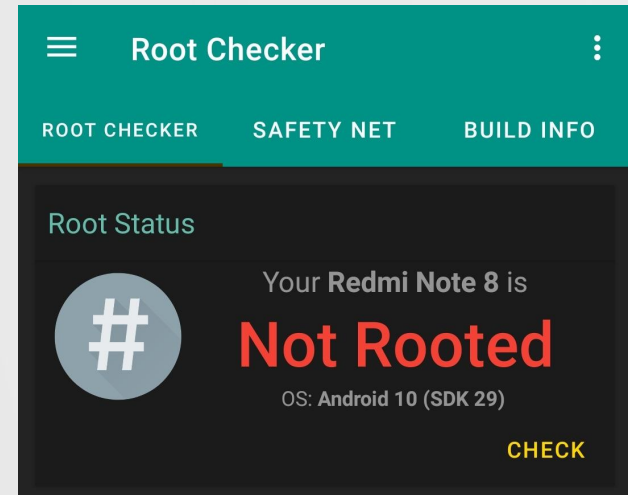


1.7 No rootee su dispositivo

Rootear su dispositivo Android rompe las restricciones de nivel de usuario impuestas por el sistema operativo Android. Esto abre significativamente el dispositivo para permitir literalmente cualquier acción privilegiada. Esto pone al dispositivo en un riesgo mucho mayor porque cualquier vulnerabilidad puede explotarse sin restricciones. Esto también anula la garantía y las actualizaciones de seguridad futuras son problemáticas de instalar.

Pasos:

- Instalar alguna aplicación y chequear si está rooteado.

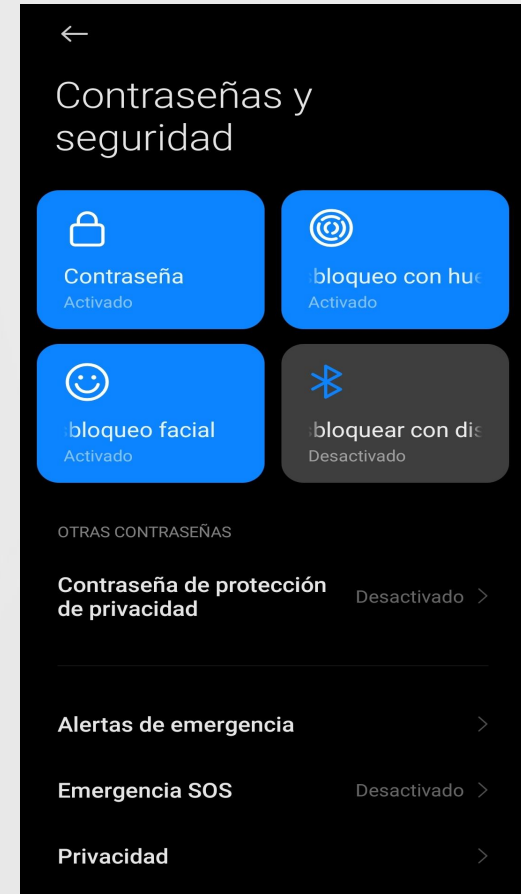


1.8 Asegúrese de que 'Smart Lock' esté configurado en 'Disabled'

Smart Lock detecta la presencia del dispositivo y sus circunstancias y lo mantiene automáticamente desbloqueado incluso si el dispositivo tiene una contraseña de pantalla, un PIN o un patrón habilitados. Como práctica recomendada, no configure el dispositivo para que se desbloquee automáticamente.

Pasos:

- Ajustes
- Contraseñas y seguridad



1.9 Asegúrese de que 'Bloquear tarjeta SIM' esté configurado en 'Habilitado'

Un PIN de la tarjeta SIM bloquea la SIM y evita que alguien retire la tarjeta SIM de su dispositivo y la use en cualquier otro dispositivo.

Pasos:

- Ajustes
- Contraseñas y seguridad
- Privacidad
- Bloqueo SIM
- Activar "Bloquear la tarjeta SIM"

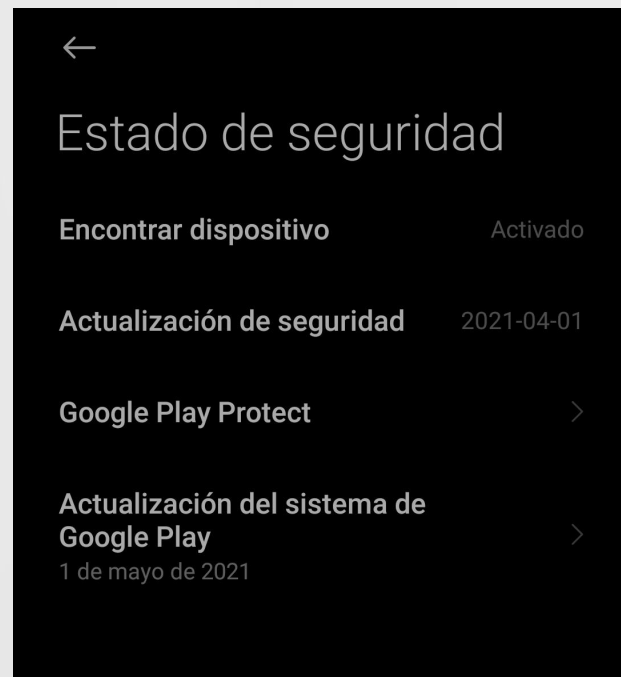


1.10 Asegúrese de que 'Buscar mi dispositivo' esté configurado en 'Habilitado'

Si pierde su dispositivo Android, puede usar Encuentra mi dispositivo para encontrar su dispositivo y también hacer sonar, bloquear o borrar los datos de su dispositivo de forma remota.

Pasos:

- Ajustes
- Estado de seguridad
- Verificar que Encontrar Dispositivo se encuentre "activado".

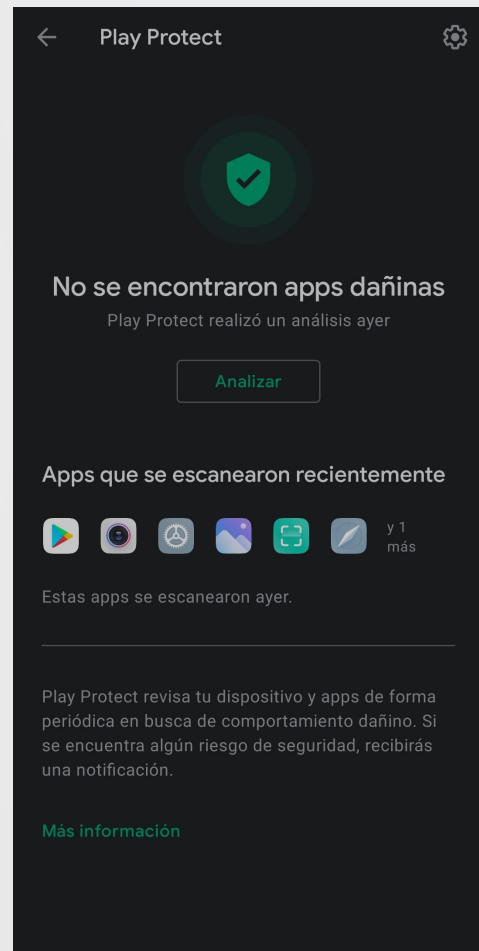
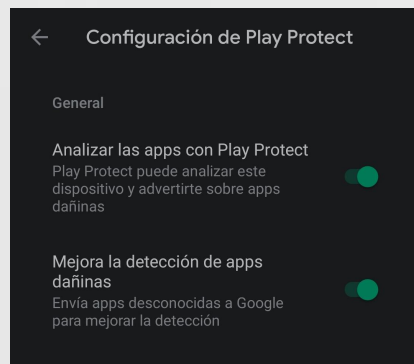


1.11 Asegúrese de que 'Analizar el dispositivo en busca de amenazas de seguridad' esté configurado como 'Habilitado'

La configuración permite que Google revise regularmente su dispositivo y prevenga o advierta sobre posibles daños.

Pasos:

- Ajustes
- Estado de seguridad
- Google Play Protect
- Verificar en ajustes que las opciones se encuentren activadas.

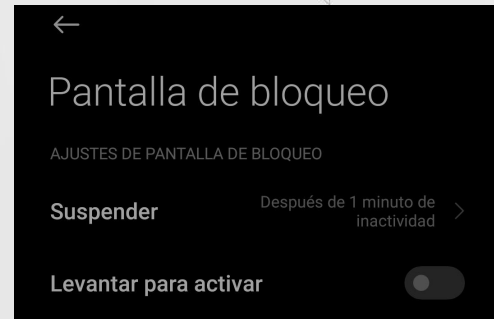


1.12 Asegúrese de que el 'Tiempo de espera de la pantalla' esté configurado en '1 minuto o menos'

Debe establecer el tiempo de espera de inactividad para evitar el uso no autorizado del dispositivo si lo deja desatendido.

Pasos:

- Ajustes
- Pantalla de bloqueo
- Verificar que "Suspende" se encuentre dentro de los valores recomendados.





02

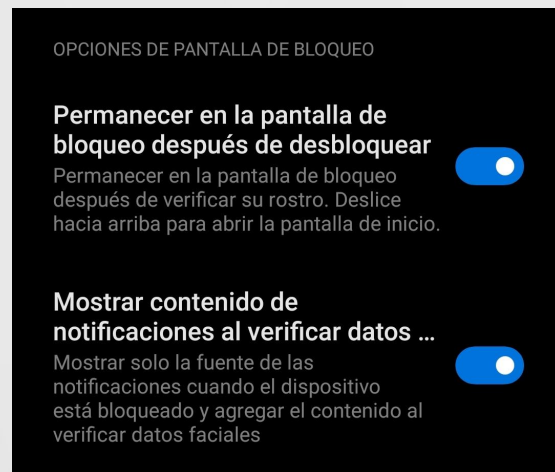
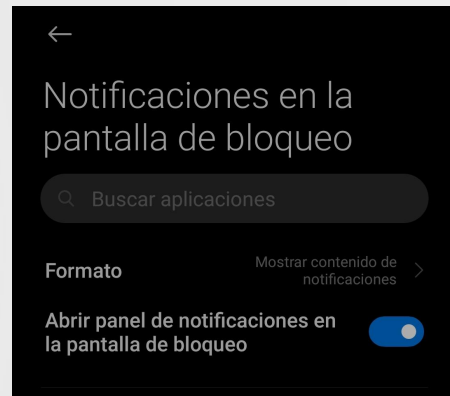
Configuración de privacidad

2.1 Asegúrese de que 'Pantalla de bloqueo' esté configurada en 'No mostrar notificaciones en absoluto'.

Si el dispositivo se pierde o está desatendido, la desactivación de las notificaciones no muestra ninguna información de notificación en la pantalla bloqueada.

Pasos:

- Ajustes
- Notificaciones
- Notificaciones en la pantalla de desbloqueo
- Verificar que en formato diga “No mostrar contenido de notificaciones”

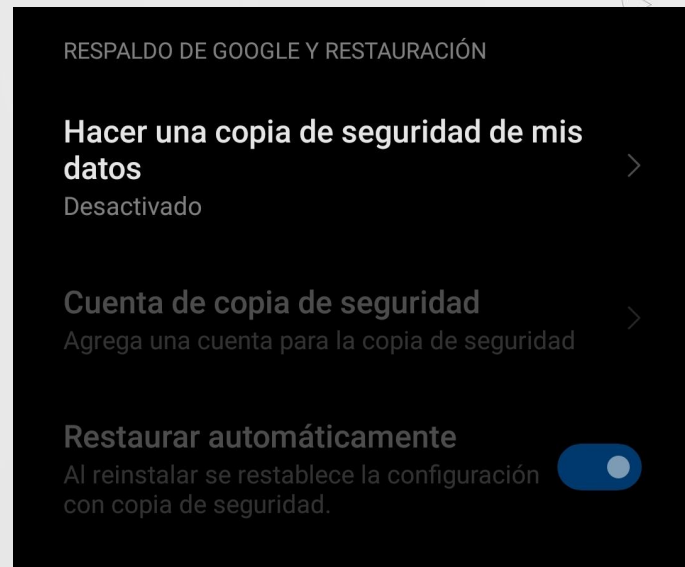


2.2 Asegúrese de que 'Copia de seguridad en Google Drive' está 'Deshabilitado'

Debido a problemas de privacidad, no se recomienda hacer una copia de seguridad de los datos personales, como mensajes de texto, correos electrónicos, fotos y contactos a terceros, a menos que acepte el riesgo de compartir los datos con un tercero.

Pasos:

- Ajustes
- Acerca del teléfono
- Hacer copia de seguridad y restaurar
- Verificar "Hacer copia de seguridad de mis datos" diga Desactivado.

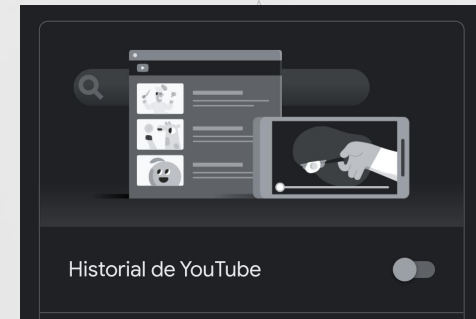
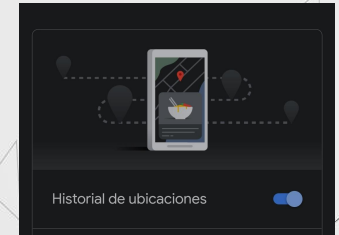
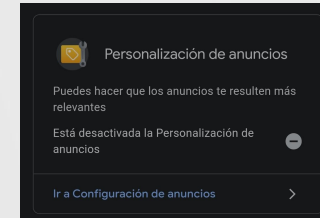
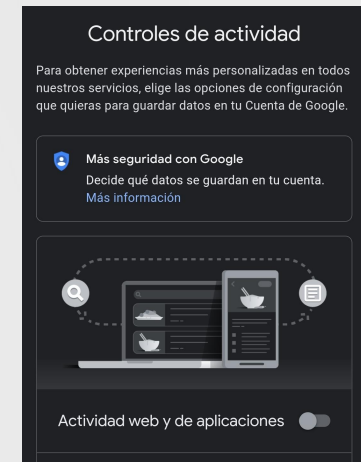



2.3 Asegúrese de que todo en la cuenta de google en el apartado 'Controles de actividad' esté configurado como 'Deshabilitado'

Esto podría ser una invasión de la privacidad y, por lo tanto, se recomienda deshabilitar estas configuraciones.

Pasos:

- Ajustes
- Privacidad
- Controles de actividad
- Seleccionar cuenta de google
- Verificar que las casilla de "Actividad web y de aplicaciones", "Historial de youtube", "Historial de ubicaciones" y Personalización de anuncios no está marcada.





03

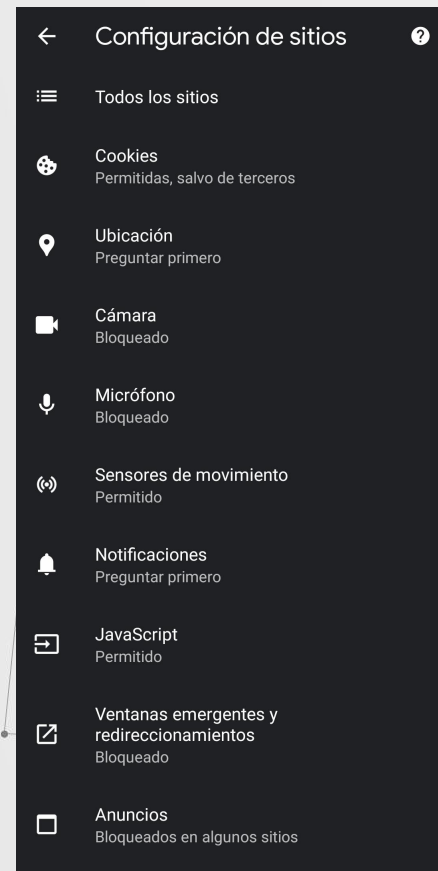
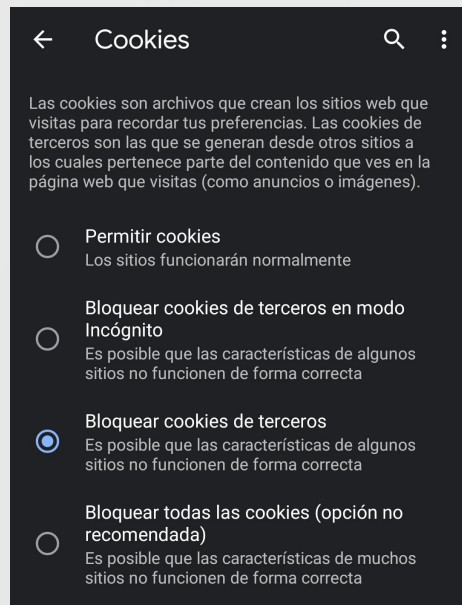
Configuración del navegador Chrome

3.1 Asegúrese de que los apartados de configuración de sitios tengan los valores recomendados.

Los sitios web deberán solicitar permiso antes de que se les permita acceder al micrófono, a la ubicación, la cámara, etc lo que ayudará a evitar el acceso no deseado y ayudará a protegerse contra posibles problemas de privacidad.

Pasos:

- Entrar a Google Chrome
- Configuración
- Configuración avanzada
- Configuración de sitios.

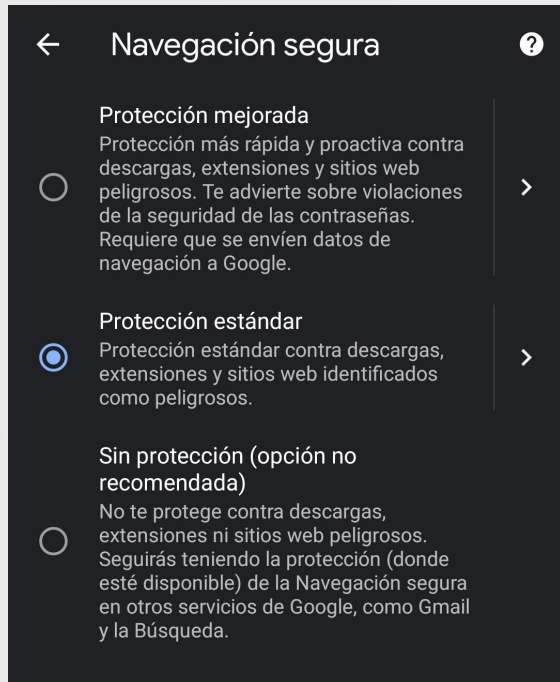


3.2 Asegúrese de que 'Navegación segura' esté configurada como 'Habilitada'

La navegación segura de Google ayuda a proteger los dispositivos todos los días al mostrar advertencias a los usuarios cuando intentan navegar a sitios peligrosos o descargar archivos peligrosos.

Pasos:

- Entrar a Google Chrome
- Configuración
- Configuración de sitios.

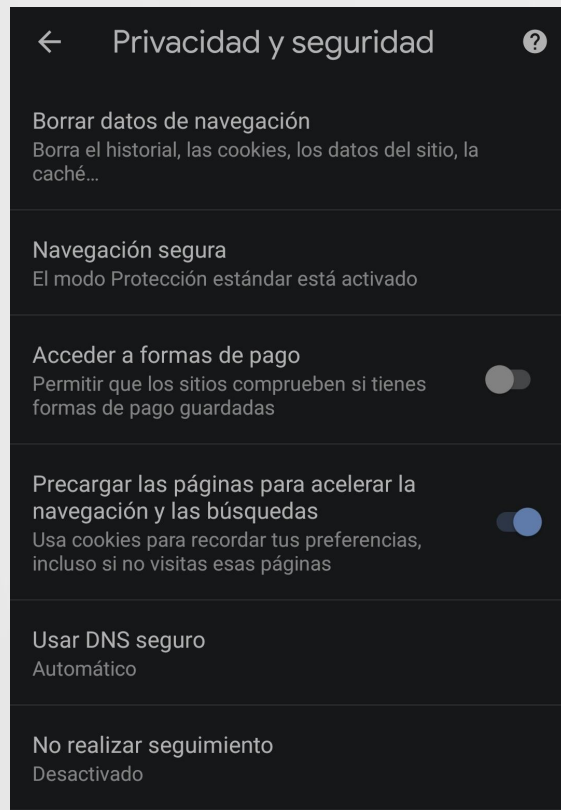


3.3 Asegúrese de que 'No rastrear' esté configurado en 'Habilitado'

Cuando navega por la web en computadoras o dispositivos Android, puede enviar una solicitud a sitios web para que no recopilen ni rastreen sus datos de navegación.

Pasos:

- Entrar a Google Chrome
- Configuración
- Privacidad y seguridad
- No realizar seguimiento
- Verificar que esté activado





Gracias

CREDITS: This presentation template was created by **Slidesgo**, including icons by **Flaticon**, and infographics & images by **Freepik**.

Please keep this slide for attribution.