Universidad del Caribe
2000 CANCUN, QUINTANA ROO, MÉXICO
CONOCIMIENTO Y CULTURA PARA EL DESARROLLO HUMANO

CIS BENCHMARK GOOGLE CHROME

SEGURIDAD DE DATOS

Alumno: Gary Izanami Gonzalez Lara
Profesor: Ismael Jimenez Sanchez

Contenido

Introducción 8

Recomendaciones 8

Enforced defautls 8

Esta sección contiene recomendaciones que se configuran de forma predeterminada al instalar Google Chrome. La aplicación de esta configuración a nivel empresarial puede evitar que esta configuración cambie a una opción menos segura. 8

1.1 HTTP authentication 8

1.1.1 (L1) Ensure 'Cross-origin HTTP Authentication prompts' is set to 'Disabled' (Automated) 8

1.2 Safe Browsing settings 9

1.2.1 (L1) Ensure 'Configure the list of domains on which Safe Browsing will not trigger warnings' is set to 'Disabled' (Automated) 9

1.2.2 (L1) Ensure 'Safe Browsing Protection Level' is set to 'Enabled: Safe Browsing is active in the standard mode.' or higher (Manual) 12

1.3 (L1) Ensure 'Allow Google Cast to connect to Cast devices on all IP addresses' is set to 'Disabled' (Automated) 13

1.4 (L1) Ensure 'Allow queries to a Google time service' is set to 'Enabled' (Automated) 14

1.5 (L1) Ensure 'Allow the audio sandbox to run' is set to 'Enabled' (Automated) ... 15

1.6 (L1) Ensure 'Ask where to save each file before downloading' is set to 'Enabled' (Automated) 17

1.7 (L1) Ensure 'Continue running background apps when Google Chrome is closed' is set to 'Disabled' (Automated) 17

1.8 (L2) Ensure 'Control SafeSites adult content filtering' is set to 'Enabled: Filter top level sites (but not embedded iframes) for adult content' (Automated) 19

1.9 (L1) Ensure 'Determine the availability of variations' is set to 'Enable all variations' (Manual) 20

1.10 (L1) Ensure 'Disable Certificate Transparency enforcement for a list of Legacy Certificate Authorities' is set to 'Disabled' (Automated) 22

1.11 (L1) Ensure 'Disable Certificate Transparency enforcement for a list of subjectPublicKeyInfo hashes' is set to 'Disabled' (Automated) 23

1.12 (L1) Ensure 'Disable Certificate Transparency enforcement for a list of URLs' is set to 'Disabled' (Automated) 24

1.13 (L1) Ensure 'Disable saving browser history' is set to 'Disabled' (Automated) . 25

1.14 (L1) Ensure 'DNS interception checks enabled' is set to 'Enabled' (Automated) 27

1.15 (L1) Ensure 'Enable component updates in Google Chrome' is set to 'Enabled' (Automated) 28

1.16 (L1) Ensure 'Enable globally scoped HTTP auth cache' is set to 'Disabled' (Automated) 29

1.17 (L1) Ensure 'Enable online OCSP/CRL checks' is set to 'Disabled' (Automated) 31

1.18 (L1) Ensure 'Enable security warnings for command-line flags' is set to 'Enabled' (Automated) 32

1.19 (L1) Ensure 'Enable third party software injection blocking' is set to 'Enabled' (Automated) 33

1.20 (L1) Ensure 'Enables managed extensions to use the Enterprise Hardware Platform API' is set to 'Disabled' (Automated) 34

1.21 (L1) Ensure 'Ephemeral profile' is set to 'Disabled' (Automated) 35

1.22 (L1) Ensure 'Import autofill form data from default browser on first run' is set to 'Disabled' (Automated) 37

1.23 (L1) Ensure 'Import of homepage from default browser on first run' is set to 'Disabled' (Automated) 38

1.24 (L1) Ensure 'Import search engines from default browser on first run' is set to 'Disabled' (Automated) 39

1.25 (L1) Ensure 'List of names that will bypass the HSTS policy check' is set to 'Disabled' (Automated) 40

1.26 (L1) Ensure 'Origins or hostname patterns for which restrictions on insecure origins should not apply' is set to 'Disabled' (Automated) 42

1.27 (L1) Ensure 'Suppress lookalike domain warnings on domains' is set to 'Disabled' (Automated) 42

1.28 (L1) Ensure 'Suppress the unsupported OS warning' is set to 'Disabled' (Automated) 44

1.29 (L1) Ensure 'URLs for which local IPs are exposed in WebRTC ICE candidates' is set to 'Disabled' (Automated) 45

2 Attack Surface Reduction 46

2.1 Update settings (Google section of GPO) 46

2.1.1 (L1) Ensure 'Update policy override' is set to 'Enabled' with 'Always allow updates (recommended)' or 'Automatic silent updates' specified (Automated) 47

2.2 Content settings 48

2.2.1 (L1) Ensure 'Control use of insecure content exceptions' is set to 'Enabled: Do not allow any site to load mixed content' (Automated) 48

2.2.2 (L2) Ensure 'Control use of the Web Bluetooth API' is set to 'Enabled: Do not allow any site to request access to Bluetooth devices via the Web Bluetooth API' (Automated) 49

2.2.3 (L2) Ensure 'Control use of the WebUSB API' is set to 'Enabled: Do not allow any site to request access to USB devices via the WebUSB API' (Automated) 51

2.2.4 (L2) Ensure 'Default notification setting' is set to 'Enabled: Do not allow any site to show desktop notifications' (Automated) 52

2.2.5 (L1) Ensure 'Allow local file access to file:// URLs on these sites in the PDF Viewer' Is Disabled (Automated) 54

2.3 Extensions 55

2.3.1 (L1) Ensure 'Blocks external extensions from being installed' is set to 'Enabled' (Automated) 55

2.3.2 (L1) Ensure 'Configure allowed app/extension types' is set to 'Enabled: extension, hosted_app, platform_app, theme' (Automated) 56

2.3.3 (L1) Ensure 'Configure extension installation blocklist' is set to 'Enabled: *' (Automated) 58

2.3.4 (L2) Ensure 'Default third-party storage partitioning setting' Is Enabled and Blocked (Automated) 59

2.3.5 (L1) Ensure 'Block third-party storage partitioning for these origins' Is Configured (Manual) 61

2.3.6 (L2) Ensure 'Control Manifest v2 extension availability' Is Set to Forced Only (Automated) 62

2.3.7 (L1) Ensure 'Control availability of extensions unpublished on the Chrome Web Store' Is Disabled (Automated) 63

2.4 HTTP authentication 65

2.4.1 (L2) Ensure 'Supported authentication schemes' is set to 'Enabled: ntlm, negotiate' (Automated) 65

2.5 Native Messaging 66

2.5.1 (L2) Ensure 'Configure native messaging blocklist' is set to 'Enabled: *' (Automated) 66

2.6 Password manager 68

2.6.1 (L1) Ensure 'Enable saving passwords to the password manager' is Explicitly Configured (Manual) 68

2.7 Printing 69

2.7.1 (L1) Ensure 'Enable Google Cloud Print Proxy' is set to 'Disabled' (Automated) 69

2.8 Remote access (Chrome Remote Desktop) 70

2.8.1 Ensure 'Allow remote access connections to this machine' is set to 'Disabled' (Manual) 70

2.8.2 (L1) Ensure 'Allow remote users to interact with elevated windows in remote assistance sessions' is set to 'Disabled' (Automated) 72

2.8.3 (L1) Ensure 'Configure the required domain names for remote access clients' is set to 'Enabled' with a domain defined (Manual) 73

2.8.4 (L1) Ensure 'Enable curtaining of remote access hosts' is set to 'Disabled' (Automated) 74

2.8.5 (L1) Ensure 'Enable firewall traversal from remote access host' is set to 'Disabled' (Automated) 76

2.8.6 (L1) Ensure 'Enable or disable PIN-less authentication for remote access hosts' is set to 'Disabled' (Automated) 77

2.8.7 (L1) Ensure 'Enable the use of relay servers by the remote access host' is set to 'Disabled'. (Automated) 79

2.9 First-Party Sets Settings 80

2.9.1 (L1) Ensure 'Enable First-Party Sets' Is Disabled (Manual) 80

2.10 Microsoft Active Directory Management Settings..... 81

2.10.1 (L1) Ensure 'Allow automatic sign-in to Microsoft cloud identity providers' Is Enabled (Manual)..... 81

2.11 (L1) Ensure 'Allow download restrictions' is set to 'Enabled: Block malicious downloads' (Automated) 82

2.12 (L2) Ensure 'Allow proceeding from the SSL warning page' is set to 'Disabled' (Automated) 83

2.13 (L1) Ensure 'Disable proceeding from the Safe Browsing warning page' is set to 'Enabled' (Automated) 84

2.14 (L1) Ensure 'Require Site Isolation for every site' is set to 'Enabled' (Automated) 85

2.15 (L2) Ensure 'Force Google SafeSearch' is set to 'Enabled' (Automated)..... 87

2.16 (L1) Ensure 'Notify a user that a browser relaunch or device restart is recommended or required' is set to 'Enabled: Show a recurring prompt to the user indication that a relaunch is required' (Automated) 88

2.17 (L1) Ensure 'Proxy settings' is set to 'Enabled' and does not contain "ProxyMode": "auto_detect" (Automated) 90

2.18 (L2) Ensure 'Require online OCSP/CRL checks for local trust anchors' is set to 'Enabled' (Automated) 92

2.19 (L1) Ensure 'Set the time period for update notifications' is set to 'Enabled: 86400000' (Automated) 93

2.20 (L1) Ensure 'Allow Web Authentication requests on sites with broken TLS certificates' Is Disabled (Automated) 95

2.21 (L1) Ensure 'Allow reporting of domain reliability related data' Is Disabled (Automated) 96

2.22 (L1) Ensure 'Enable TLS Encrypted ClientHello' Is Enabled (Automated) 97

2.23 (L2) Ensure 'Determines whether the built-in certificate verifier will enforce constraints encoded into trust anchors loaded from the platform trust store' Is Enabled (Automated) 99

2.24 (L1) Ensure 'Keep browsing data when creating enterprise profile by default' Is Enabled (Automated) 100

2.25 (L1) Ensure 'Allow file or directory picker APIs to be called without prior user gesture' Is Disabled (Automated)..... 101

2.26 (L1) Ensure 'Enable Google Search Side Panel' Is Disabled (Automated)..... 103

2.27 (L1) Ensure 'Http Allowlist' Is Properly Configured (Manual)..... 104

2.28 (L1) Ensure 'Enable automatic HTTPS upgrades' Is Enabled (Automated) 105

2.29 (L1) Ensure 'Insecure Hashes in TLS Handshakes Enabled' Is Disabled (Automated) 107

2.30 (L1) Ensure 'Enable Renderer App Container' Is Enabled (Automated)..... 107

2.31 (L1) Ensure 'Enable strict MIME type checking for worker scripts' Is Enabled (Automated) 109

2.32 Ensure 'Allow remote debugging' is set to 'Disabled' (Automated)..... 110

3 Privacy 111

3.1 Content settings..... 111

3.1.1 (L2) Ensure 'Default cookies setting' is set to 'Enabled: Keep cookies for the duration of the session' (Automated)..... 111

3.1.2 (L1) Ensure 'Default geolocation setting' is set to 'Enabled: Do not allow any site to track the users' physical location' (Automated) 113

3.2 Google Cast..... 115

3.2.1 (L1) Ensure 'Enable Google Cast' is set to 'Disabled' (Automated)..... 115

3.3 (L1) Ensure 'Allow websites to query for available payment methods' is set to 'Disabled' (Automated) 116

3.4 (L1) Ensure 'Block third party cookies' is set to 'Enabled' (Automated)..... 117

3.5 (L2) Ensure 'Browser sign in settings' is set to 'Enabled: Disabled browser sign-in' (Automated) 118

3.6 (L1) Ensure 'Control how Chrome Cleanup reports data to Google' is set to 'Disabled' (Automated) 120

3.7 (L1) Ensure 'Disable synchronization of data with Google' is set to 'Enabled' (Automated) 121

3.8 (L1) Ensure 'Enable alternate error pages' is set to 'Disabled' (Automated).... 122

3.9 (L1) Ensure 'Enable deleting browser and download history' is set to 'Disabled' (Automated) 123

3.10 (L1) Ensure 'Enable predict network actions` is set to 'Enabled: Do not predict actions on any network connection' (Automated) 124

3.11 (L1) Ensure 'Enable or disable spell checking web service' is set to 'Disabled' (Automated) 126

3.12 (L1) Ensure 'Enable reporting of usage and crash-related data' is set to 'Disabled' (Automated) 127

3.13 (L1) Ensure 'Enable Safe Browsing for trusted sources' is set to 'Disabled' (Automated) 128

3.14 (L2) Ensure 'Enable search suggestions' is set to 'Disabled' (Automated)..... 130

3.15 (L2) Ensure 'Enable Translate' is set to 'Disabled' (Automated) 131

3.16 (L1) Ensure 'Enable URL-keyed anonymized data collection' is set to 'Disabled' (Automated) 132

4 Data Loss Prevention 133

4.1 Allow or deny screen capture 133

4.1.1 (L2) Ensure 'Allow or deny screen capture' is set to 'Disabled' (Automated) 133

4.2 Content settings..... 135

4.2.1 (L2) Ensure 'Control use of the Serial API' is set to 'Enabled: Do not allow any site to request access to serial ports via the Serial API' (Automated)..... 135

4.2.2 (L2) Ensure 'Default Sensors Setting' is set to 'Enabled: Do not allow any site to access sensors' (Automated) 137

4.2.3 (L1) Ensure 'Allow clipboard for these sites' Is Configured (Manual) 138

4.2.4 (L1) Ensure 'Block clipboard on these sites' Is Configured (Manual) 139

4.2.5 (L1) Ensure 'Default clipboard setting' Is 'Enabled' to 'Deny Permissions' (Automated) 141

4.2.6 (L2) Ensure 'Default Window Management permissions setting' Is 'Enabled' to 'Deny Permission' (Automated)..... 143

4.2.7 (L2) Ensure 'Allow Window Management permission on these sites' Is Configured (Manual)..... 144

4.2.8 (L2) Ensure 'Block Window Management permission on these sites' Is Configured (Manual)..... 146

4.3 (L2) Ensure 'Allow invocation of file selection dialogs' is set to 'Disabled' (Automated) 147

4.4 (L2) Ensure 'Allow or deny audio capture' is set to 'Disabled' (Automated) 148

4.5 (L2) Ensure 'Allow or deny video capture' is set to 'Disabled' (Automated)..... 150

4.6 (L1) Ensure 'Allow user feedback' is set to 'Disabled' (Automated)..... 151

4.7 (L2) Ensure 'Controls the mode of DNS-over-HTTPS' is set to 'Enabled: DNS-over-HTTPS without insecure fallback' (Automated) 153

4.8 (L2) Ensure 'Enable AutoFill for addresses' is set to 'Disabled' (Automated) ... 154

4.9 (L1) Ensure 'Enable AutoFill for credit cards' is set to 'Disabled' (Automated) . 155

4.10 (L1) Ensure 'Import saved passwords from default browser on first run' is set to 'Disabled' (Automated) 156

4.11 (L1) Ensure 'List of types that should be excluded from synchronization' is set to 'Enabled: passwords' (Automated) 158

4.12 (L2) Ensure 'Allow or deny screen capture' is set to 'Disabled' (Automated) . 159

5 Forensics (Post Incident)..... 160

5.1 (L2) Ensure 'Enable guest mode in browser' is set to 'Disabled' (Automated) . 160

5.2 (L2) Ensure 'Incognito mode availability' is set to 'Enabled: Incognito mode disabled' (Automated) 162

5.3 (L1) Ensure 'Set disk cache size, in bytes' is set to 'Enabled: 250609664' (Automated) 163

Conclusión 165

Introducción

En la era digital actual, la seguridad en línea se ha convertido en una prioridad absoluta. Cada día, millones de personas utilizan navegadores como **Google Chrome** para navegar por la vastedad de la web. Sin embargo, esta comodidad también puede exponernos a diversas amenazas en línea, como virus y hackers.

Para combatir estos riesgos, existe un recurso invaluable: el manual "**CIS Benchmark for Google Chrome**". Este manual, elaborado por un grupo dedicado a la seguridad en internet, ofrece una gran cantidad de consejos y recomendaciones para fortalecer la seguridad de Chrome.

En este proyecto, nuestro objetivo es seguir estos consejos de manera sistemática. Nuestra meta es configurar Chrome de tal manera que esté robustamente protegido contra amenazas en línea, pero sin comprometer su facilidad de uso. Acompáñanos en este viaje para hacer de la navegación en internet una experiencia más segura.

Recomendaciones

ENFORCED DEFAUTLS

Esta sección contiene recomendaciones que se configuran de forma predeterminada al instalar Google Chrome. La aplicación de esta configuración a nivel empresarial puede evitar que esta configuración cambie a una opción menos segura.

1.1 HTTP AUTHENTICATION

1.1.1 (L1) ENSURE 'CROSS-ORIGIN HTTP AUTHENTICATION PROMPTS' IS SET TO 'DISABLED' (AUTOMATED)

Descripción: Esta configuración controla si el su contenido de terceros puede abrir un cuadro de diálogo de autenticación básica HTTP y, por lo general, está deshabilitada. El estado recomendado para esta configuración es: Deshabilitado (0)

Justificación: Esta configuración suele estar deshabilitada para ayudar a combatir los intentos de suplantación de identidad (phishing).

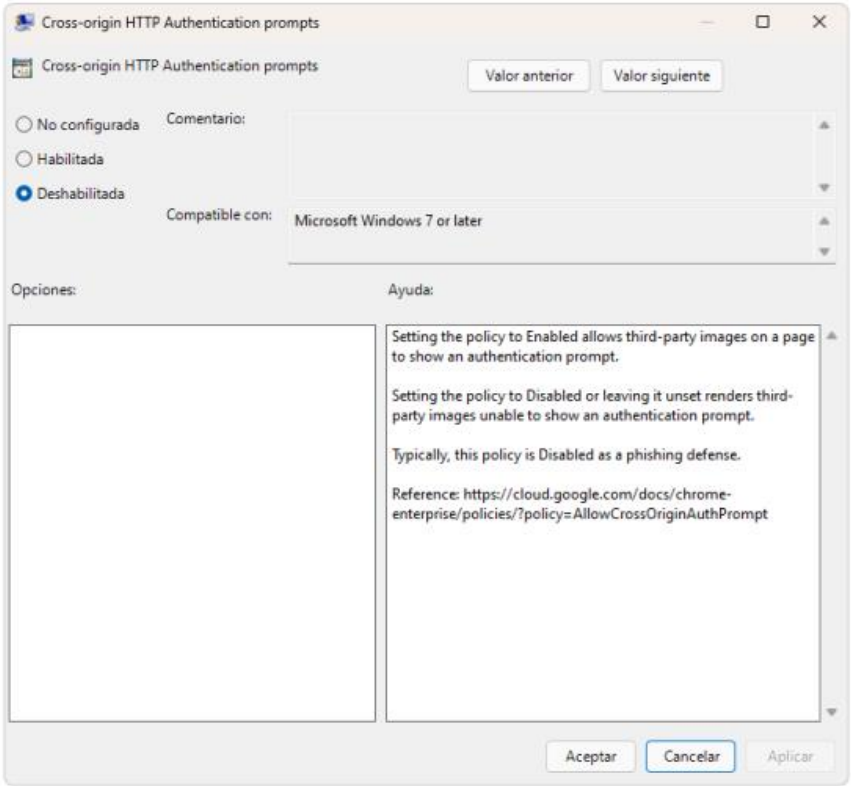
Impacto: Ninguno: este es el comportamiento predeterminado.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:AllowCrossOriginAuthPrompt
```

Corrección: Para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Deshabilitada:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\HTTP authentication\Cross-origin HTTP Authentication prompts
```



1.2 Safe Browsing settings

1.2.1 (L1) Ensure 'Configure the list of domains on which Safe Browsing will not trigger warnings' is set to 'Disabled' (Automated)

Descripción: La configuración determina la funcionalidad de la navegación segura. Deshabilitado (0): la protección de Navegación segura se aplica a todos los recursos Habilitado (1), con una lista de 1 o más sitios: significa que Navegación segura confiará

en los dominios que designe. No los comprobará en busca de recursos peligrosos como phishing, malware o software no deseado

El estado recomendado para esta configuración es: Deshabilitado (0)

NOTA: El servicio de protección de descargas de Navegación segura no comprobará las descargas alojadas en estos dominios y su servicio de protección con contraseña no comprobará la reutilización de contraseñas.

Justificación: La navegación segura de Google ayudará a proteger a los usuarios de una variedad de sitios maliciosos y fraudulentos, o de descargar archivos peligrosos.

Impacto: Ninguno: este es el comportamiento predeterminado.

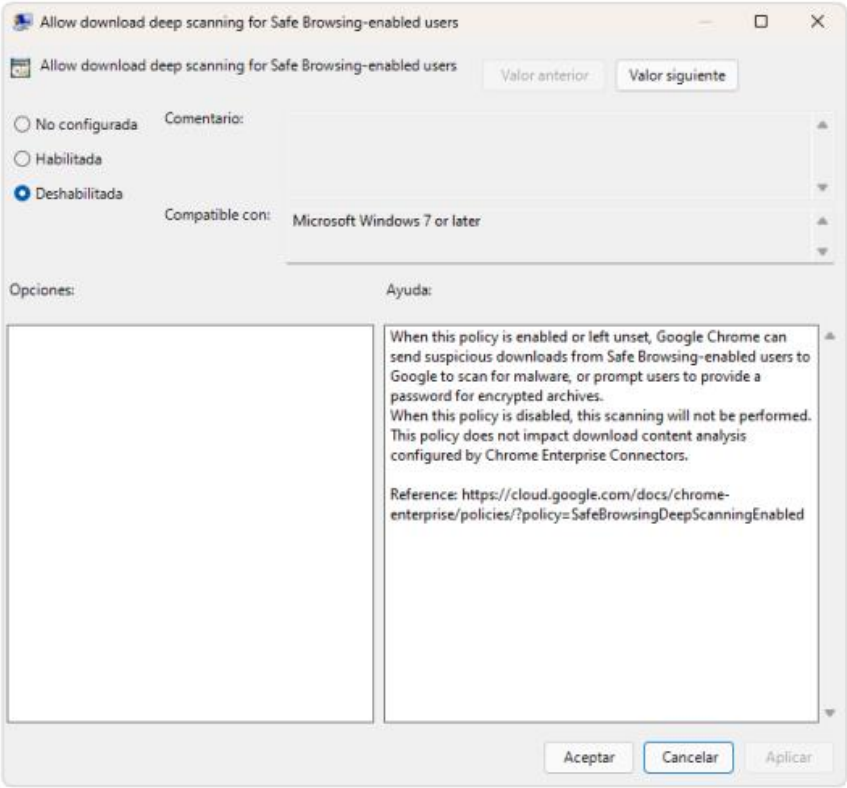
NOTA: El único impacto real es la posible molestia del usuario si va a un sitio legítimo que se considera falsamente fraudulento (una ocurrencia rara). Esto se puede manejar agregando el sitio a la lista de permitidos y/o notificando a Google sobre el hallazgo falso.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta ruta de acceso del Registro no existirá si se establece en Deshabilitado:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\SafeBrowsingAllowlistDomai
ns\
```

Corrección: Para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Deshabilitada:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\Safe Browsing settings\Configure the list of domains on which Safe
Browsing will not trigger warnings.
```


Allow download deep scanning for Safe Browsing-enabled users
Allow download deep scanning for Safe Browsing-enabled users
Valor anterior
Valor siguiente
No configurada
Habilitada
Deshabilitada
Comentario:
Compatible con:
Microsoft Windows 7 or later
Opciones:
Ayuda:
When this policy is enabled or left unset, Google Chrome can send suspicious downloads from Safe Browsing-enabled users to Google to scan for malware, or prompt users to provide a password for encrypted archives.
When this policy is disabled, this scanning will not be performed.
This policy does not impact download content analysis configured by Chrome Enterprise Connectors.
Reference: https://cloud.google.com/docs/chrome-enterprise/policies/?policy=SafeBrowsingDeepScanningEnabled
Aceptar
Cancelar
Aplicar

1.2.2 (L1) Ensure 'Safe Browsing Protection Level' is set to 'Enabled: Safe Browsing is active in the standard mode.' or higher (Manual)

Descripción: Controla si la función de navegación segura de Google Chrome está habilitada y el modo en el que funciona. Si estableces esta configuración como obligatoria, los usuarios no podrán cambiar ni anular la configuración de Navegación segura en Google Chrome. Si esta configuración no se establece, la navegación segura funcionará en el modo de protección estándar, pero los usuarios pueden cambiar esta configuración.

- Sin protección (0): Navegación segura nunca está activa.
- Protección estándar (1): La navegación segura está activa en el modo estándar.
- Protección mejorada (2): La navegación segura está activa en el modo mejorado. Este modo proporciona una mayor seguridad, pero requiere compartir más información de navegación con Google.

El estado recomendado para esta configuración es: Navegación segura está activa en el modo estándar. (1) o alto

Justificación: La navegación segura de Google ayudará a proteger a los usuarios de una variedad de sitios maliciosos y fraudulentos, o de la descarga de archivos peligrosos.

NOTA: Google recomienda utilizar el modo de navegación segura mejorada (2). Activar la navegación segura mejorada aumentará sustancialmente la protección contra sitios web y descargas peligrosos, pero compartirá más datos con Google.

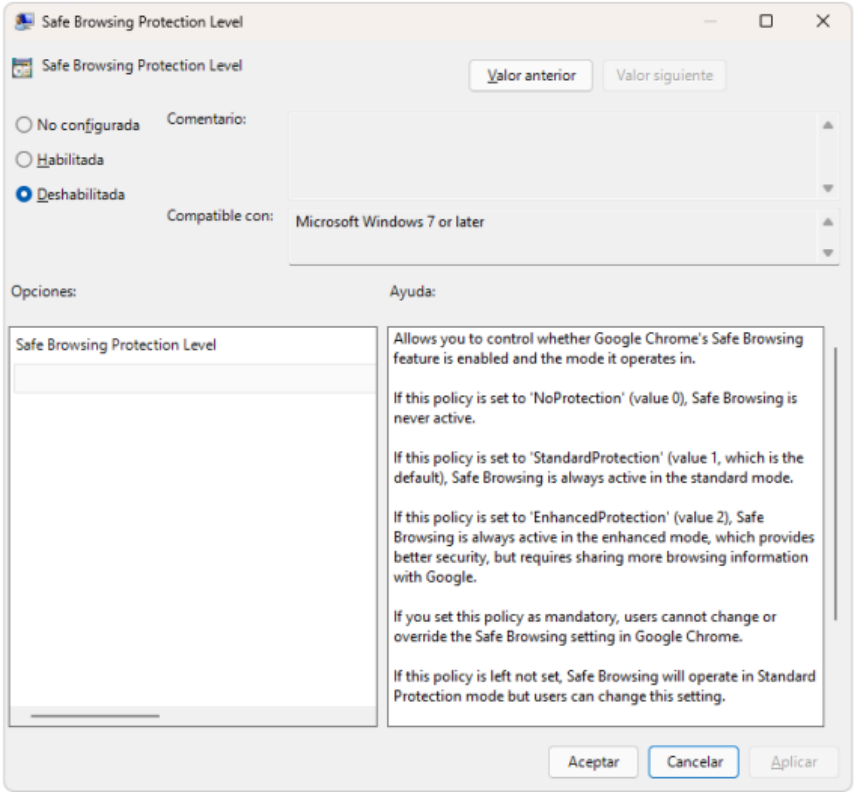
Impacto: Ninguno: este es el comportamiento predeterminado (protección estándar).

Auditoría: Navegue hasta la ruta de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 1 o 2:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:SafeBrowsingProtectionLeve
l
```

Corrección: Para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Habilitada: Navegación segura está activa en el modo estándar:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\Safe Browsing settings\Safe Browsing Protection Level
```



1.3 (L1) Ensure 'Allow Google Cast to connect to Cast devices on all IP addresses' is set to 'Disabled' (Automated)

Descripción: Esta configuración controla si Google Cast puede conectarse a todas las direcciones IP o solo a las direcciones IP privadas, tal como se define en RFC1918 (IPv4) y RFC4193 (IPv6). Tenga en cuenta que, si la configuración de EnabledMediaRouter se establece en Deshabilitado, no hay ningún efecto positivo o negativo para esta configuración.

El estado recomendado para esta configuración es: Deshabilitado (0)

Justificación: Permitir que Google Cast se conecte a direcciones IP públicas podría permitir que los medios y otros datos potencialmente confidenciales se expongan al público. Si inhabilitas esta configuración, te asegurarás de que Google Cast solo pueda conectarse a direcciones IP privadas (es decir, internas).

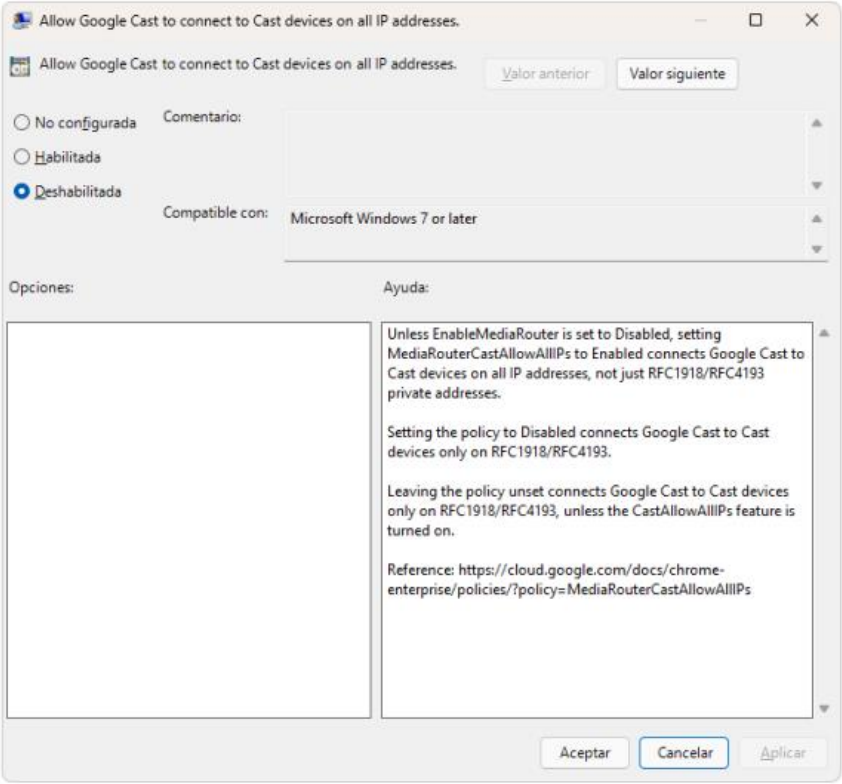
Impacto: Ninguno: este es el comportamiento predeterminado.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:MediaRouterCastAllowAllIPs
```

Corrección: Para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Deshabilitada:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\Google Cast\Allow Google Cast to connect to Cast devices on all IP
addresses.
```



1.4 (L1) Ensure 'Allow queries to a Google time service' is set to 'Enabled' (Automated)

Descripción: Esta configuración controla si Google Chrome puede enviar consultas a un servicio de hora de Google para obtener marcas de tiempo precisas. Esta comprobación ayuda en la validación de los certificados. El estado recomendado para esta configuración es: Habilitado (1)

Justificación: Google Chrome utiliza un servicio de hora de red para realizar un seguimiento aleatorio de las horas de un servicio externo de confianza. Esto permite a Google Chrome la capacidad de verificar la validez de un certificado y es importante para la validación del certificado.

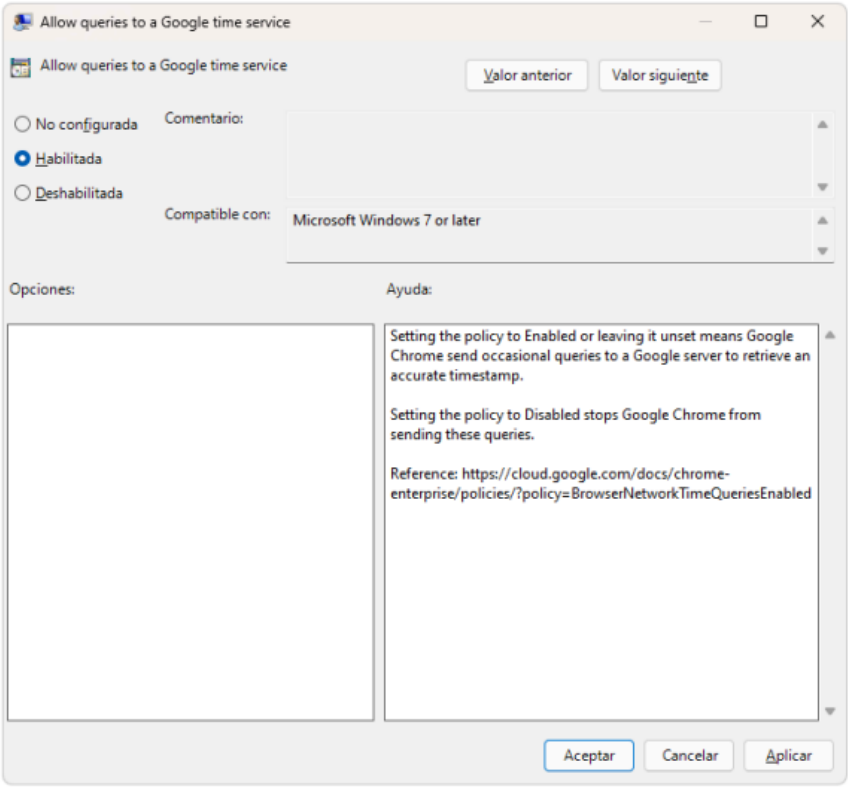
Impacto: Ninguno: este es el comportamiento predeterminado.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 1:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:BrowserNetworkTimeQueriesE
nabled
```

Corrección: Para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Habilitada:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\Allow queries to a Google time service
```



1.5 (L1) Ensure 'Allow the audio sandbox to run' is set to 'Enabled' (Automated)

Descripción: Esta configuración controla si los procesos de audio de Google Chrome se ejecutan en un entorno aislado.

NOTA: Las configuraciones de software de seguridad dentro de su entorno pueden interferir con el espacio aislado.

El estado recomendado para esta configuración es: Habilitado (1)

Justificación: Hacer que los procesos de audio se ejecuten en un espacio aislado garantiza que, si un sitio web hace un mal uso de los procesos de audio, los datos no se puedan manipular ni filtrar del sistema.

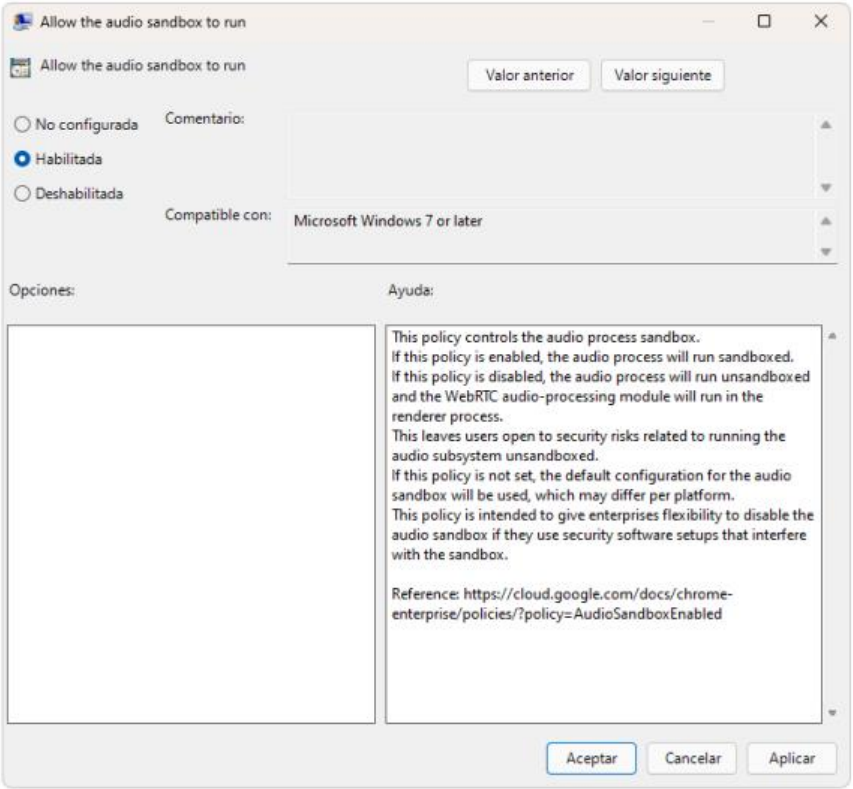
Impacto: Ninguno: este es el comportamiento predeterminado.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 1:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:AudioSandboxEnabled
```

Corrección: Para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Habilitada:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\Allow the audio sandbox to run
```



1.6 (L1) Ensure 'Ask where to save each file before downloading' is set to 'Enabled' (Automated)

Descripción: Google Chrome ofrece descargar archivos automáticamente al directorio de descargas predeterminado sin preguntar. Si esta configuración está habilitada, siempre se pregunta a los usuarios dónde guardar cada archivo antes de descargarlo. El estado recomendado para esta configuración es: Habilitado (1)

Justificación: Se debe evitar que los usuarios sufran la amenaza de descargas no autorizadas.

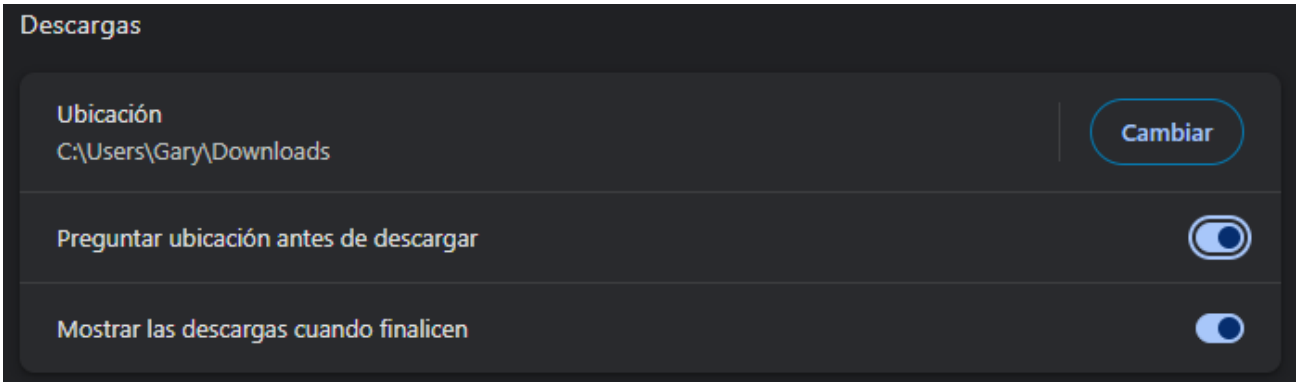
Impacto: Ninguno: Este es el comportamiento predeterminado.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 1:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:PromptForDownloadLocation
```

Corrección: Para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Habilitada:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\Ask where to save each file before downloading
```



1.7 (L1) Ensure 'Continue running background apps when Google Chrome is closed' is set to 'Disabled' (Automated)

Descripción: Chrome permite que los procesos iniciados mientras el navegador está abierto permanezcan en ejecución una vez que se haya cerrado el navegador. También permite que las aplicaciones en segundo plano y la sesión de navegación actual permanezcan activas después de cerrar el navegador.

Con esta configuración deshabilitada, el navegador cerrará sus procesos y dejará de ejecutar aplicaciones en segundo plano.

El estado recomendado para esta configuración es: Inhabilitado (0)

Justificación: Si esta configuración está habilitada, los complementos, las aplicaciones y los procesos vulnerables o maliciosos pueden seguir ejecutándose incluso después de que Chrome se haya cerrado.

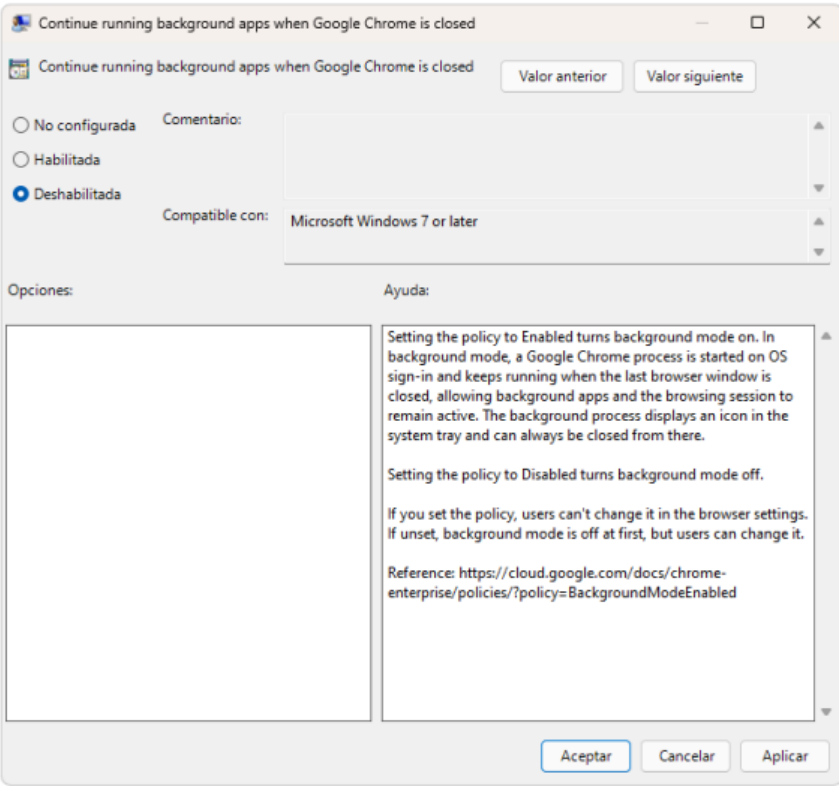
Impacto: Ninguno: este es el comportamiento predeterminado.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:BackgroundModeEnabled
```

Corrección: Para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Deshabilitada:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\Continue running background apps when Google Chrome is closed
```



1.8 (L2) Ensure 'Control SafeSites adult content filtering' is set to 'Enabled: Filter top level sites (but not embedded iframes) for adult content' (Automated)

Descripción: Google Chrome puede utilizar la API de Búsqueda segura de Google para clasificar las URL como pornográficas o no. El estado recomendado para esta configuración es: Habilitado con un valor de Filtrar sitios de nivel superior (pero no iframes incrustados) para contenido para adultos (1)

Justificación: Permitir que los resultados de búsqueda presenten sitios que puedan tener contenido malintencionado debe prohibirse para ayudar a garantizar que los usuarios no visiten accidentalmente sitios que son más propensos a contenido malintencionado, incluido el spyware. adware y virus.

Impacto: Se filtrarán los resultados de búsqueda de los usuarios y no se mostrará contenido como texto, vídeos e imágenes para adultos.

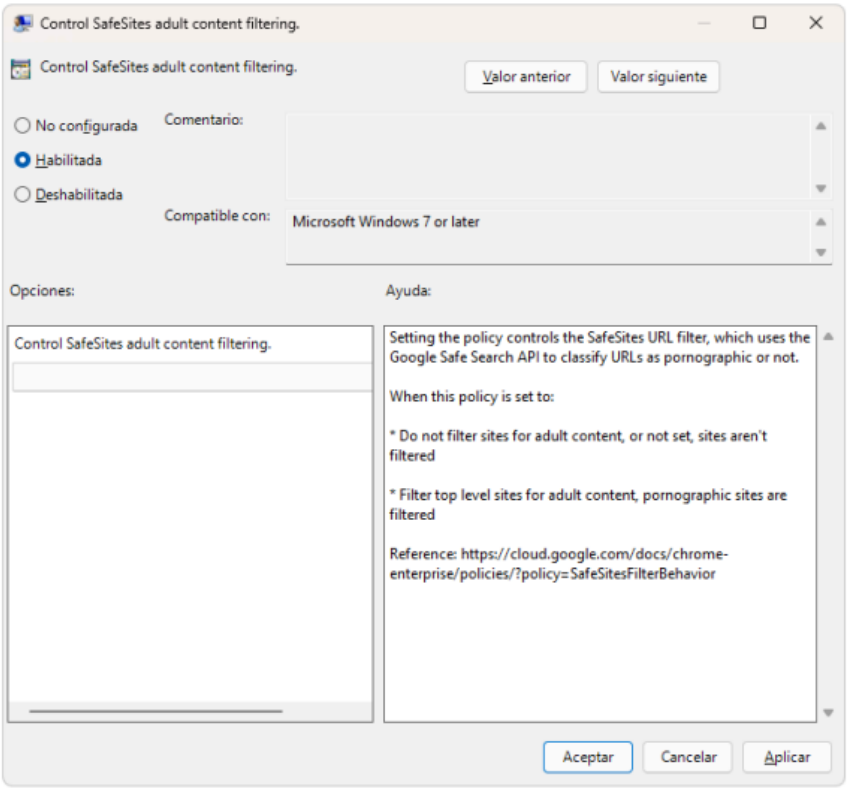
NOTA: El uso de la API de búsqueda segura de Google puede filtrar información que se escribe o pega por error en el omnibox, por ejemplo, contraseñas, servicios web internos, estructuras de carpetas, etc.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 1:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:SafeSitesFilterBehavior
```

Corrección: Para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Habilitada: No filtrar sitios por contenido para adultos:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\Control SafeSites adult content filtering.
```



1.9 (L1) Ensure 'Determine the availability of variations' is set to 'Enable all variations' (Manual)

Descripción: La configuración de esta opción permite especificar qué variaciones se pueden aplicar en Google Chrome. Las variaciones proporcionan un medio para que Google ofrezca modificaciones a Google Chrome sin enviar una nueva versión del navegador mediante la habilitación o inhabilitación selectiva de funciones ya existentes.

- Habilitar todas las variaciones (0): Permite que todas las variaciones se apliquen al navegador (valor predeterminado).
- Habilitar variaciones relacionadas solo con correcciones críticas (1): solo permite que se apliquen a Google Chrome variaciones consideradas correcciones críticas de seguridad o estabilidad.
- Desactivar todas las variaciones (2): Impide que todas las variaciones se apliquen al navegador. Tenga en cuenta que este modo puede impedir que los desarrolladores de Google Chrome proporcionen correcciones de seguridad críticas de manera oportuna y, por lo tanto, no se recomienda.

El estado recomendado para esta configuración es: Habilitar todas las variaciones (0)

NOTA: Google cree firmemente que no hay ningún beneficio de seguridad adicional por convertir esto en correcciones críticas, ya que dejarlo activado aumenta la

estabilidad del navegador. La desactivación de las variaciones también puede impedir la obtención de actualizaciones de seguridad críticas de manera oportuna.

Justificación: Google recomienda encarecidamente dejar esta configuración predeterminada (0 = Habilitar todas las variaciones), para que las correcciones se habiliten gradualmente (o, si es necesario, se deshabiliten rápidamente) a través del marco de Chrome Variaciones.

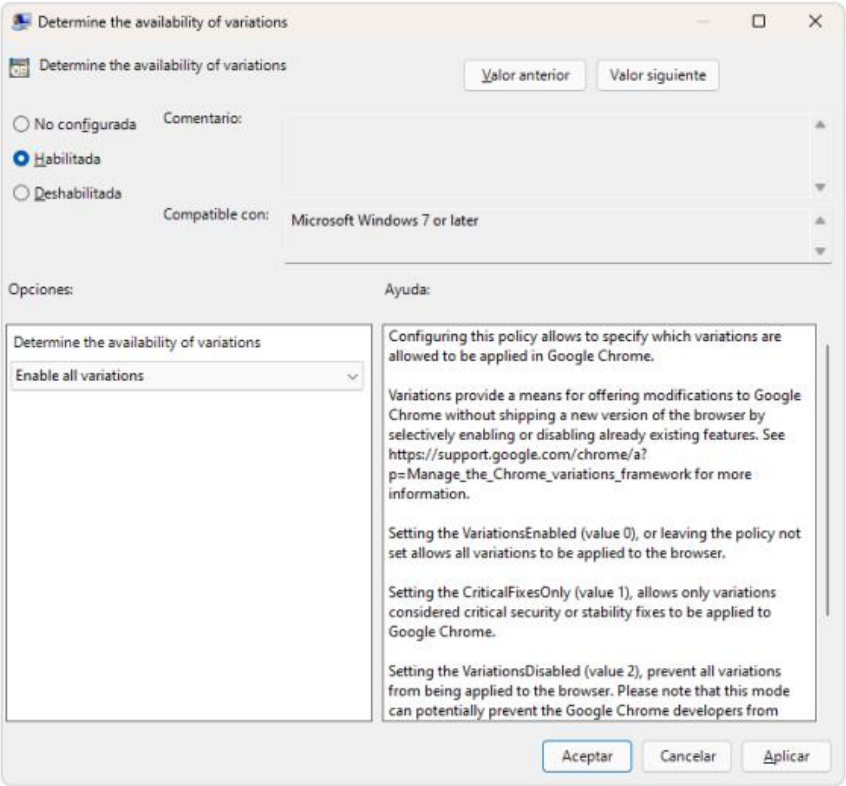
Impacto: Ninguno: este es el comportamiento predeterminado.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:ChromeVariations
```

Corrección: Para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Habilitada: Habilitar todas las variaciones:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\Determine the availability of variations
```



1.10 (L1) Ensure 'Disable Certificate Transparency enforcement for a list of Legacy Certificate Authorities' is set to 'Disabled' (Automated)

Descripción: Google Chrome puede inhabilitar la aplicación de los requisitos de transparencia de certificados para una lista de entidades de certificación heredadas. Si esta configuración está deshabilitada, los certificados que no se divulguen correctamente públicamente según lo requerido por la transparencia de certificados no son de confianza.

El estado recomendado para esta configuración es: Deshabilitado (0)

Justificación: Las autoridades de certificación heredadas deben seguir la directiva de transparencia de certificados.

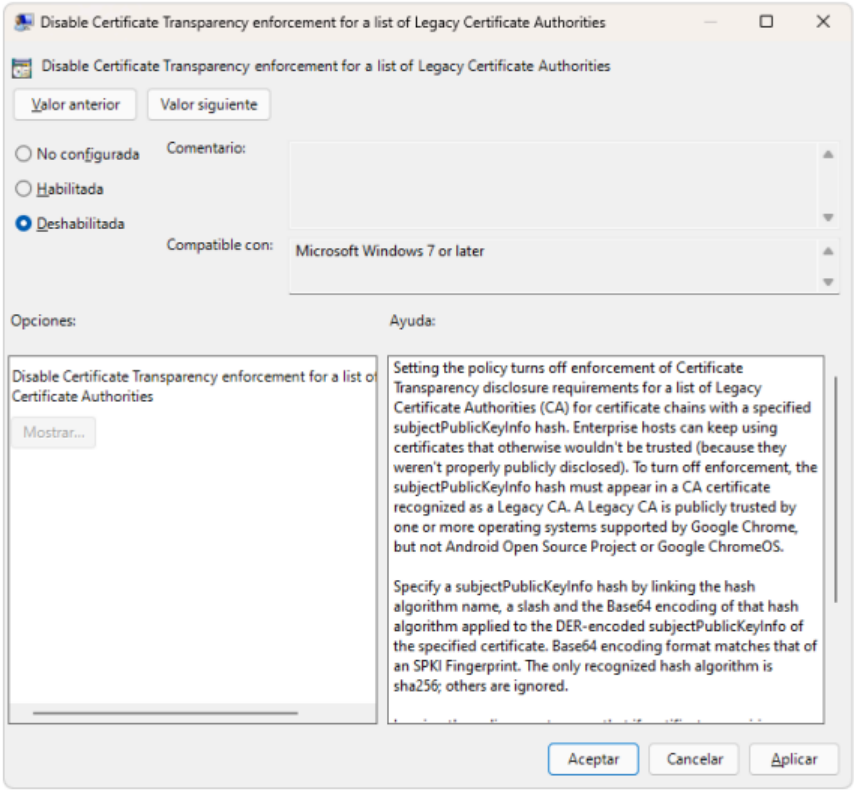
Impacto: Ninguno: este es el comportamiento predeterminado.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta ruta de acceso del Registro no existirá si se establece en Deshabilitado:

```
HKEY LOCAL MACHINE\SOFTWARE\Policies\Google\Chrome\CertificateTransparencyEnf
orcementDisabledForLegacyCas\
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Deshabilitada:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\Disable Certificate Transparency enforcement for a list of Legacy
Certificate Authorities
```



1.11 (L1) Ensure 'Disable Certificate Transparency enforcement for a list of subjectPublicKeyInfo hashes' is set to 'Disabled' (Automated)

Descripción: Google Chrome puede excluir certificados por sus hashes subjectPublicKeyInfo para que no apliquen los requisitos de transparencia de certificados. Si esta configuración está deshabilitada, no se excluye ningún certificado de los requisitos de transparencia de certificados. El estado recomendado para esta configuración es: Deshabilitado (0)

Justificación: Los requisitos de transparencia de certificados se aplicarán a todos los certificados.

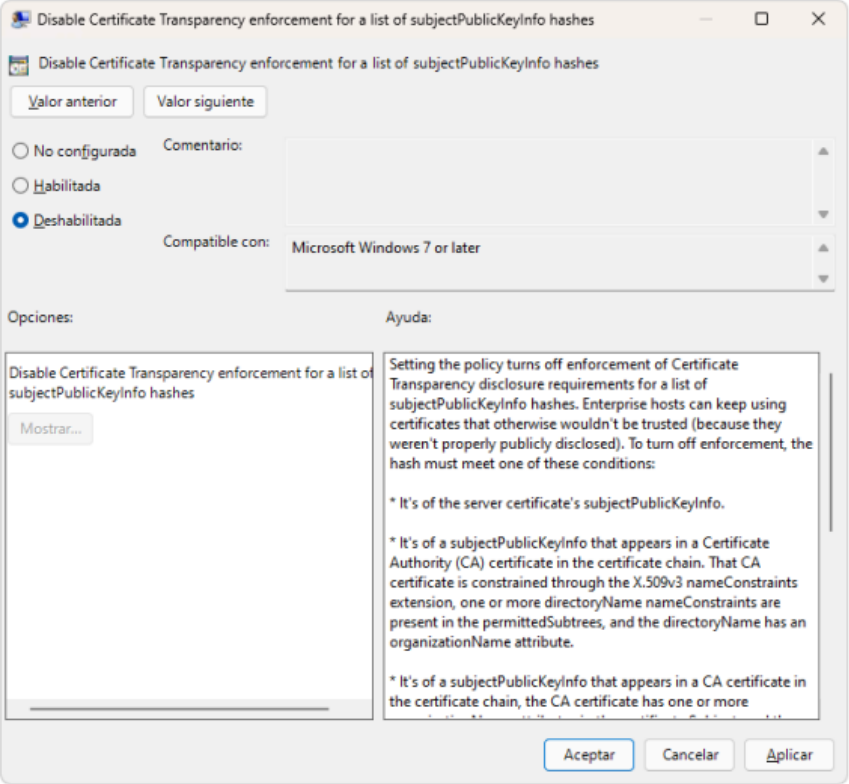
Impacto: Ninguno: este es el comportamiento predeterminado.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta ruta de acceso del Registro no existirá si se establece en Deshabilitado:

```
HKEY LOCAL MACHINE\SOFTWARE\Policies\Google\Chrome\CertificateTransparencyEnf
orcementDisabledForCas
```

Corrección: Para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Deshabilitado:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\Disable Certificate Transparency enforcement for a list of
subjectPublicKeyInfo hashes
```



1.12 (L1) Ensure 'Disable Certificate Transparency enforcement for a list of URLs' is set to 'Disabled' (Automated)

Descripción: Google Chrome puede especificar URLs o nombres de host para los que no se aplicará la transparencia de certificados. Si esta configuración está deshabilitada, no se excluye ninguna dirección URL de los requisitos de transparencia de certificados. El estado recomendado para esta configuración es: Deshabilitado (0)

Justificación: Los certificados que deben divulgarse a través de la transparencia de certificados se tratarán para todas las direcciones URL como no confiables si no se divulgan de acuerdo con la directiva de transparencia de certificados.

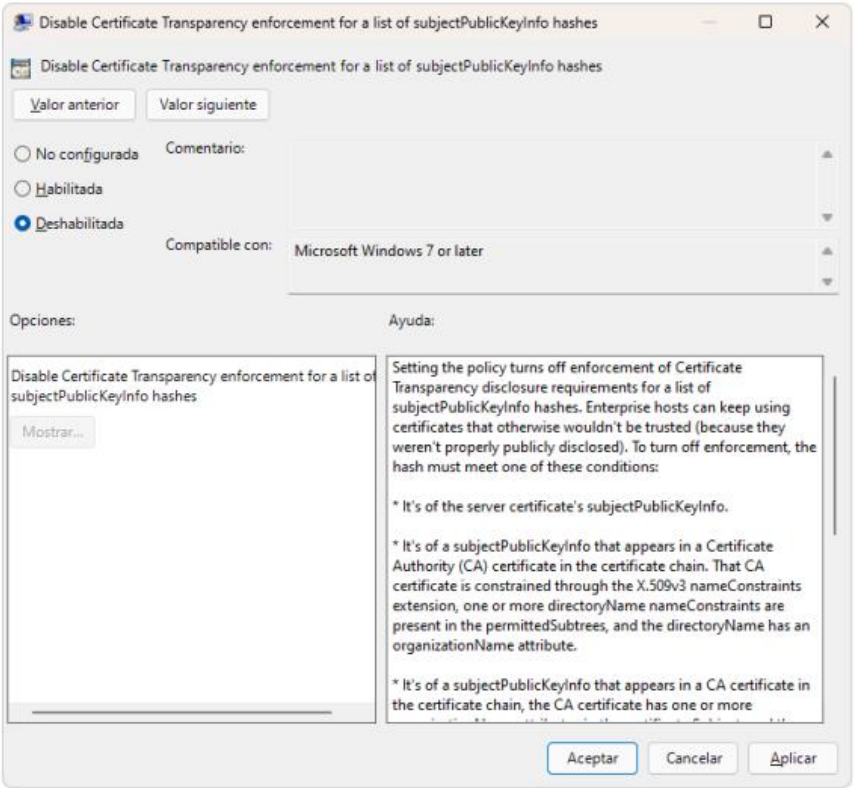
Impacto: Ninguno: este es el comportamiento predeterminado.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta ruta de acceso del Registro no existirá si se establece en Deshabilitado:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\CertificateTransparencyEnf
orcementDisabledForUrls
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Deshabilitada:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\Disable Certificate Transparency enforcement for a list of URLs
```



1.13 (L1) Ensure 'Disable saving browser history' is set to 'Disabled' (Automated)

Descripción: Google Chrome está configurado para guardar el historial del navegador. El estado recomendado para esta configuración es: Deshabilitado (0)

NOTA: Esta configuración conservará el historial de navegación que podría contener el historial de navegación personal de un usuario. Asegúrese de que esta configuración cumpla con las políticas de la organización.

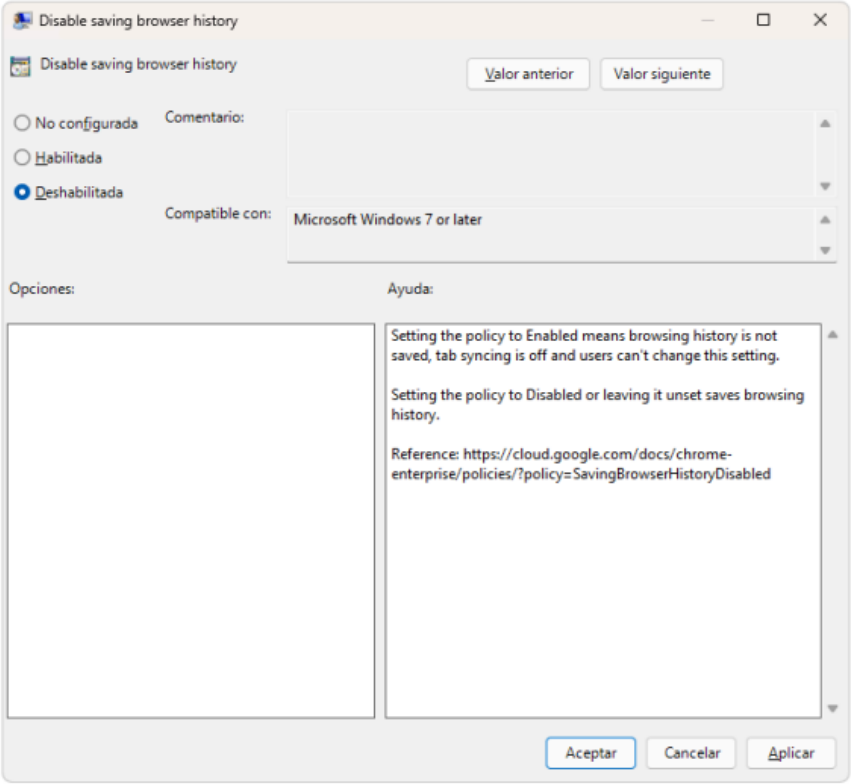
Justificación: Se guardará el historial del navegador, ya que puede contener indicadores de compromiso. Impacto: Ninguno: este es el comportamiento predeterminado.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:SavingBrowserHistoryDisabl
ed
```

Corrección: Para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Deshabilitada:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\Disable saving browser history
```



1.14 (L1) Ensure 'DNS interception checks enabled' is set to 'Enabled' (Automated)

Descripción: Esta configuración determina si un conmutador local está configurado para las comprobaciones de interceptación de DNS. Estas comprobaciones intentan descubrir si el navegador está detrás de un proxy que redirige nombres de host desconocidos.

El estado recomendado para esta configuración es: Habilitado (1)

NOTA: Es posible que esta detección no sea necesaria en un entorno empresarial en el que se conozca la configuración de red. Se puede deshabilitar para evitar tráfico DNS y HTTP adicional al inicio y cada cambio de configuración de DNS.

Justificación: La desactivación de estas comprobaciones podría permitir el secuestro y el envenenamiento de DNS.

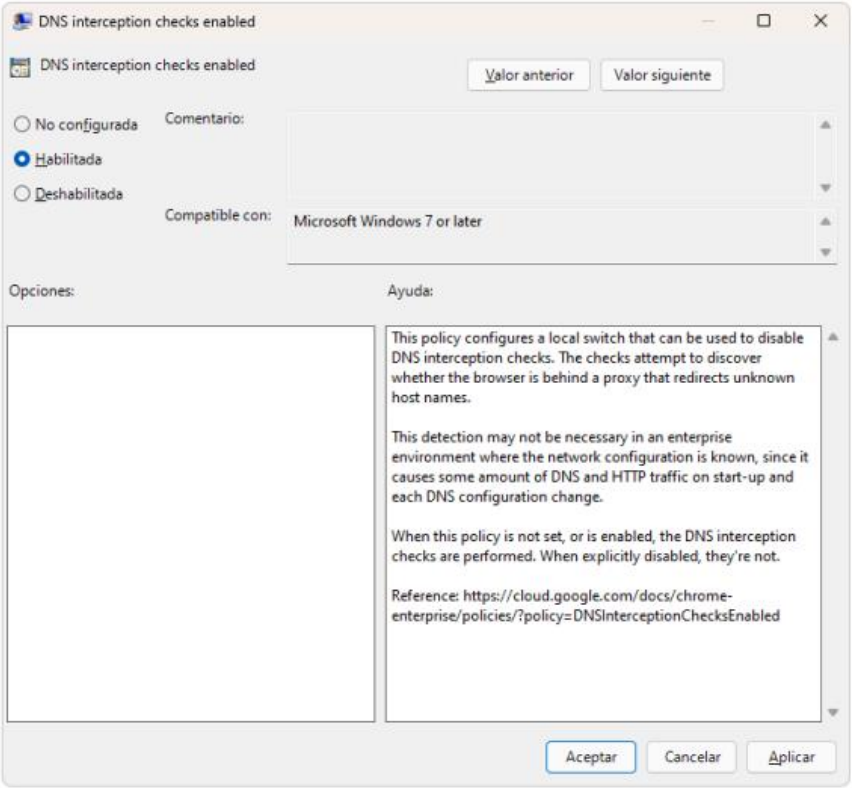
Impacto: Ninguno: este es el comportamiento predeterminado.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 1:

```
HKEY LOCAL MACHINE\SOFTWARE\Policies\Google\Chrome:DNSInterceptionChecksEnabl
ed
```

Corrección: Para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Habilitada:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\DNS interception checks enabled
```



1.15 (L1) Ensure 'Enable component updates in Google Chrome' is set to 'Enabled' (Automated)

Descripción: El actualizador de componentes de Google Chrome actualiza varios componentes de Google Chrome de forma periódica (solo se aplica a los componentes del navegador Chrome).

El estado recomendado para esta configuración es: Habilitado (1)

NOTA: No se deshabilitarán las actualizaciones de ningún componente que no contenga código ejecutable, que no altere significativamente el comportamiento del navegador o que sea crítico para su seguridad (por ejemplo, las listas de revocación de certificados y los datos de Navegación segura se actualizan independientemente de esta configuración). Para su información, chrome://components enumera todos los componentes, pero no si se ven afectados por esta configuración.

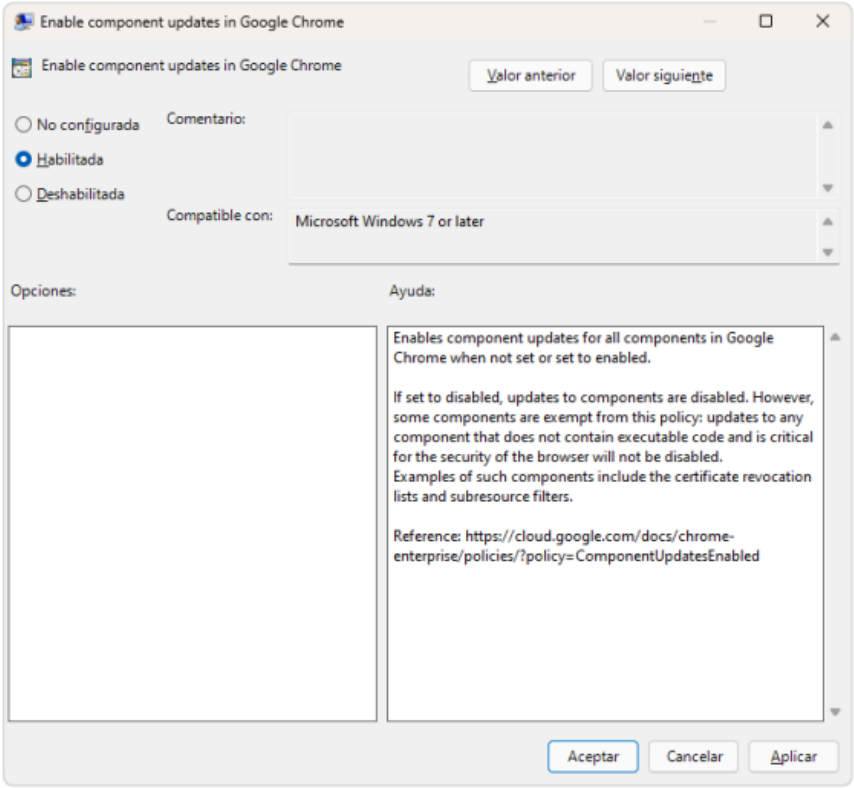
NOTA: Google proporcionó la siguiente lista de "algunos de los componentes" controlados por esta configuración:

- Componente de recuperación
- Pnacl
- Floc
- Sugerencias de optimización

- Asistente de errores SSL
- Conjunto de CRL
- Pruebas de origen
- Informador de SW
- Metadatos PKI

Justificación: Se utilizará Google Chrome Updater para mantener actualizados los componentes incluidos en Chrome.

Impacto: Ninguno: este es el comportamiento predeterminado.



1.16 (L1) Ensure 'Enable globally scoped HTTP auth cache' is set to 'Disabled' (Automated)

Descripción: esta configuración controla si las credenciales de autenticación HTTP se pueden usar automáticamente en el contexto de otro sitio web visitado en Google Chrome. El estado recomendado para esta configuración es: Deshabilitado (0)

NOTA: Esta configuración está pensada para dar a las empresas que, en función del comportamiento heredado, la oportunidad de actualizar sus procedimientos de inicio de sesión y se eliminará en el futuro.

Justificación: Permitir que las credenciales de autenticación HTTP se compartan sin el consentimiento del usuario podría llevar a que un usuario comparta información confidencial sin su conocimiento. Habilitar esta configuración también podría dar lugar a algunos tipos de ataques entre sitios que permitirían rastrear a los usuarios en todos los sitios sin el uso de cookies.

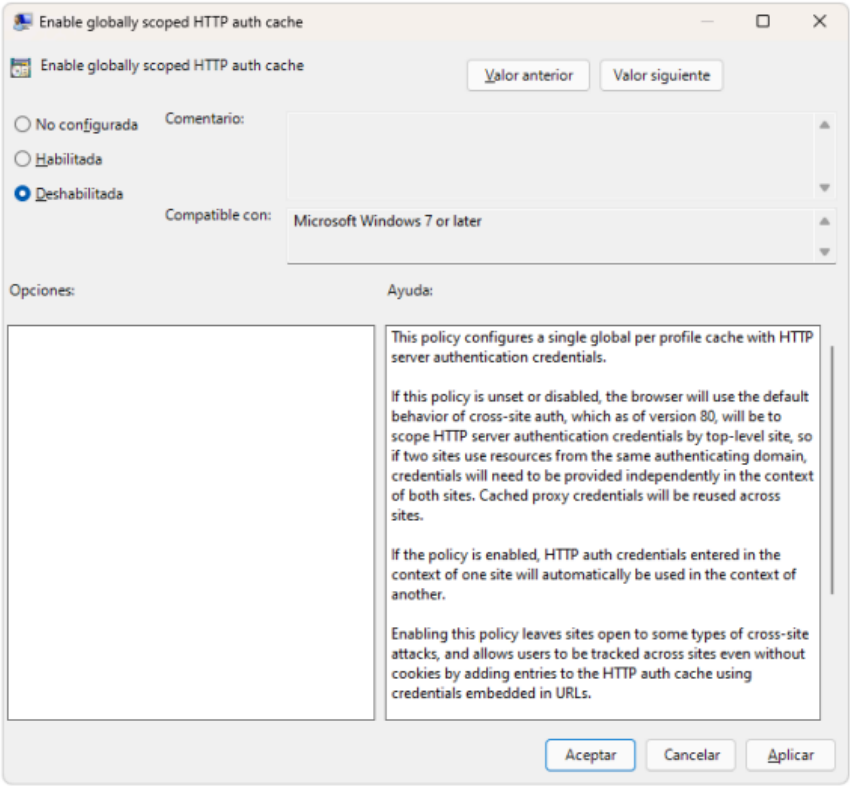
Impacto: Ninguno: este es el comportamiento predeterminado.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:GloballyScopeHTTPAuthCache
Enabled
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Deshabilitada:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\Enable globally scoped HTTP auth cache
```



1.17 (L1) Ensure 'Enable online OCSP/CRL checks' is set to 'Disabled' (Automated)

Descripción: Google Chrome puede reactivar las comprobaciones de revocación en línea con errores leves, aunque en la mayoría de los casos pueden proporcionar algún beneficio.

Si esta configuración está deshabilitada, ya no se realizan comprobaciones de OCSP/CRL en línea no seguras.

El estado recomendado para esta configuración es: Inhabilitado (0)

Justificación: Los CRLSets son principalmente un medio por el cual Chrome puede bloquear rápidamente los certificados en situaciones de emergencia. Como función secundaria, también pueden contener un cierto número de revocaciones que no sean de emergencia. Estas últimas revocaciones se obtienen mediante el rastreo de las CRL publicadas por las CA. Chrome no realiza las comprobaciones en línea (es decir, OCSP y CRL) de forma predeterminada. La biblioteca de certificados del sistema subyacente siempre realiza estas comprobaciones independientemente de lo que haga Chrome, por lo que habilitarla aquí es redundante. Un atacante puede bloquear el tráfico OCSP y hacer que se pasen las comprobaciones de revocación para provocar el uso de un comportamiento de error suave. Además, el navegador puede filtrar a los servidores de CA a qué sitio web se accede y quién accede a él.

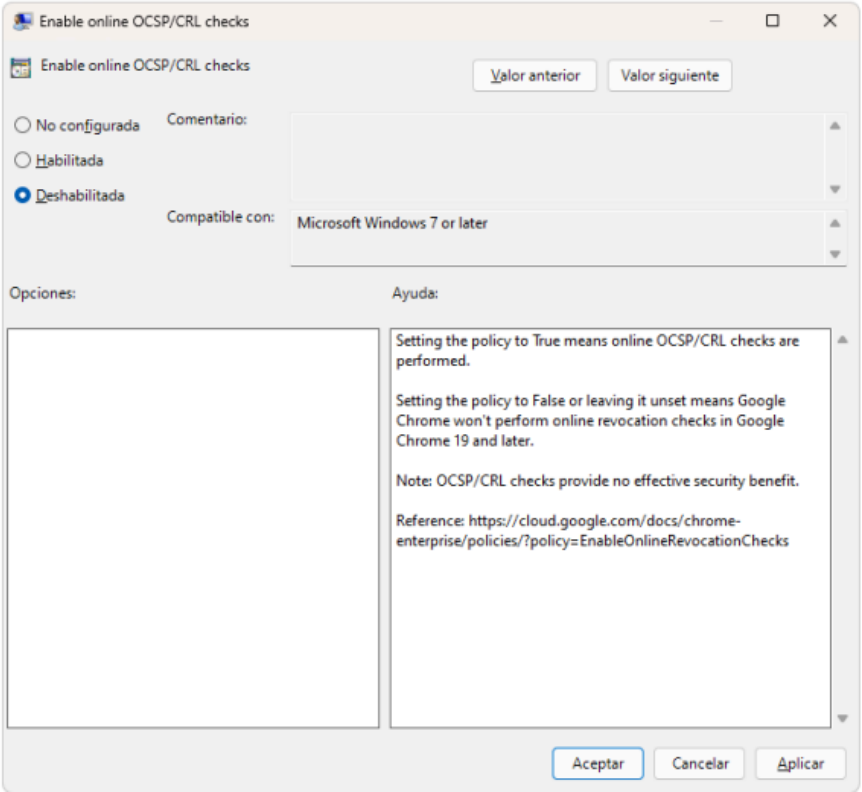
Impacto: Ninguno: este es el comportamiento predeterminado.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:EnableOnlineRevocationChec
ks
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Deshabilitada:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\Enable online OCSP/CRL checks
```



1.18 (L1) Ensure 'Enable security warnings for command-line flags' is set to 'Enabled' (Automated)

Descripción: esta configuración impide que Google Chrome muestre advertencias de seguridad que indiquen que se están utilizando indicadores de línea de comandos potencialmente peligrosos en el momento de su inicio. El estado recomendado de esta configuración es: Habilitado (0)

Justificación: Si Google Chrome se inicia con indicadores potencialmente peligrosos, esta información debe mostrarse al usuario como advertencia. De lo contrario, el usuario puede estar utilizando involuntariamente una configuración no segura y estar expuesto a fallos de seguridad.

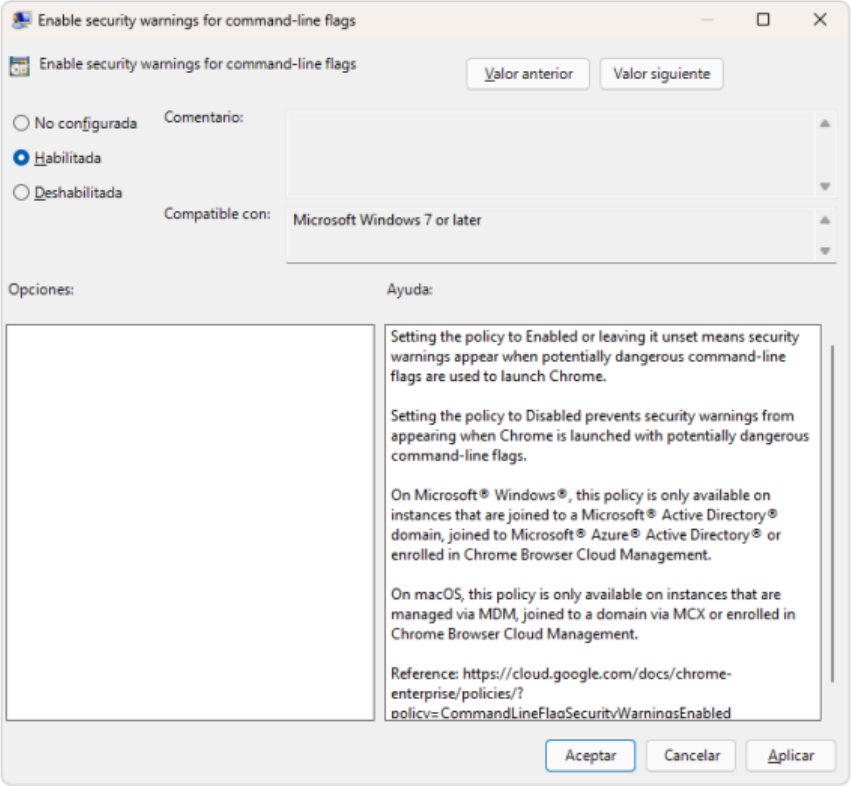
Impacto: Ninguno: este es el comportamiento predeterminado.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 1:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:CommandLineFlagSecurityWar
ningsEnabled
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Habilitada:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\Enable security warnings for command-line flags
```



1.19 (L1) Ensure 'Enable third party software injection blocking' is set to 'Enabled' (Automated)

Descripción: Google Chrome puede impedir que software de terceros inserte código ejecutable en los procesos de Chrome. El estado recomendado para esta configuración es: Habilitado (1)

Justificación: El software de terceros no podrá inyectar código ejecutable en los procesos de Chrome.

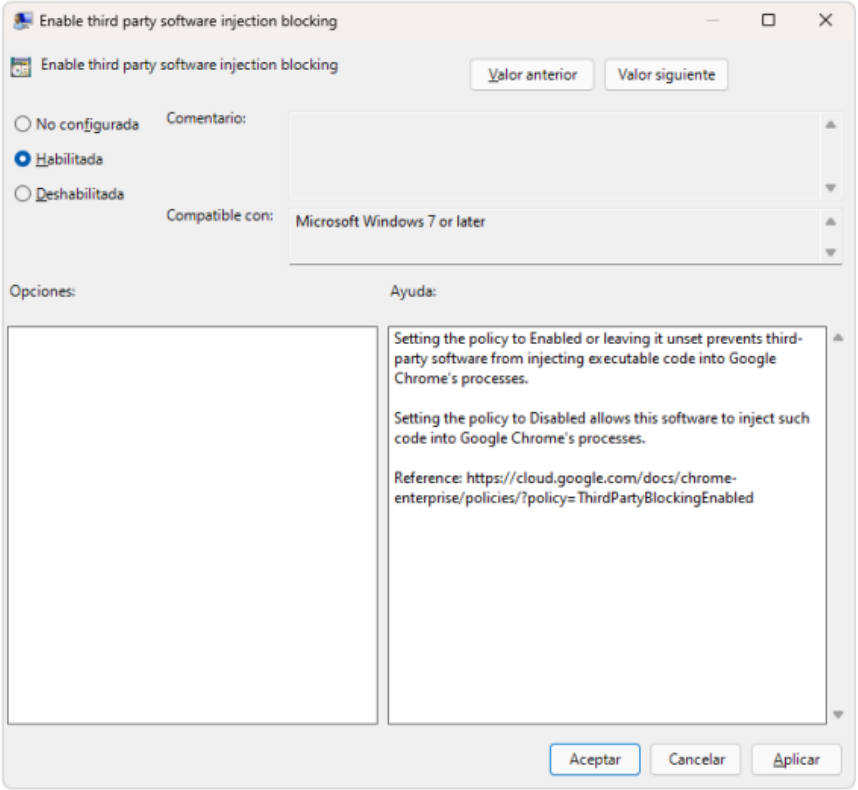
Impacto: Ninguno: este es el comportamiento predeterminado.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 1:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:ThirdPartyBlockingEnabled
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Habilitada:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\Enable third party software injection blocking
```



1.20 (L1) Ensure 'Enables managed extensions to use the Enterprise Hardware Platform API' is set to 'Disabled' (Automated)

Descripción: esta configuración permite que las extensiones instaladas por las directivas empresariales puedan utilizar la API de la plataforma de hardware empresarial. El estado recomendado para esta configuración es: Deshabilitado (0)

Justificación: Se recomienda que esta configuración esté deshabilitada a menos que las directivas de empresa indiquen lo contrario.

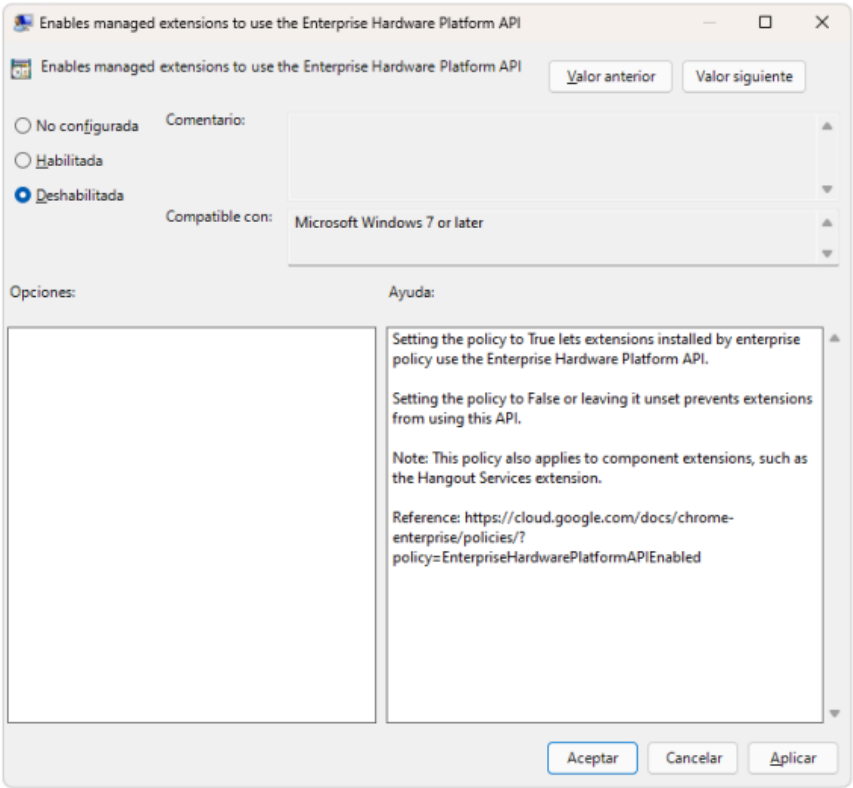
Impacto: Ninguno: este es el comportamiento predeterminado.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:EnterpriseHardwarePlatform
APIEnabled
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Deshabilitada:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\Enables managed extensions to use the Enterprise Hardware Platform API
```



1.21 (L1) Ensure 'Ephemeral profile' is set to 'Disabled' (Automated)

Descripción: esta configuración controla si los perfiles de usuario se cambian al modo efímero. En el modo efímero, los datos de perfil se guardan en el disco durante la duración de la sesión y, a continuación, los datos se eliminan una vez finalizada la sesión.

Por lo tanto, no se guardan datos en el dispositivo. El estado recomendado para esta configuración es: Deshabilitado (0)

Justificación: Permitir el uso de perfiles efímeros permite a un usuario utilizar Google Chrome sin que se registren datos en el sistema. Al eliminar los datos del navegador, se eliminará la información que puede ser importante para una investigación informática y es posible que los investigadores, como los analistas forenses informáticos, no puedan recuperar la información pertinente para la investigación.

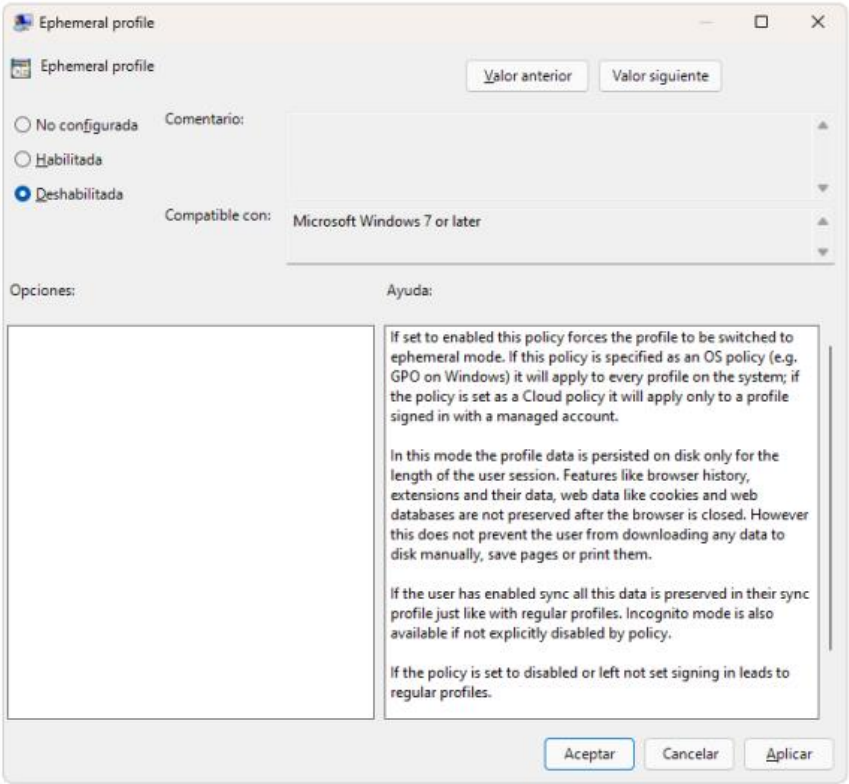
Impacto: Ninguno: este es el comportamiento predeterminado.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:ForceEphemeralProfiles
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Deshabilitada:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\Ephemeral profile
```



1.22 (L1) Ensure 'Import autofill form data from default browser on first run' is set to 'Disabled' (Automated)

Descripción: esta configuración controla si los usuarios pueden importar datos de autocompletar de otros navegadores a Google Chrome. Si estableces esta opción en Desactivado, los usuarios no podrán realizar una importación de datos de autocompletado durante la ejecución de Google Chrome. Esto también evitará que los usuarios importen datos después de que se haya configurado Google Chrome. El estado recomendado para esta configuración es: Inhabilitado (0)

Justificación: Permitir que se importen datos de autocompletar podría permitir datos confidenciales, como información de identificación personal (PII) de una fuente no segura, en Google Chrome. Teniendo en cuenta que el almacenamiento de datos confidenciales debe manejarse con cuidado, se recomienda deshabilitar esta configuración.

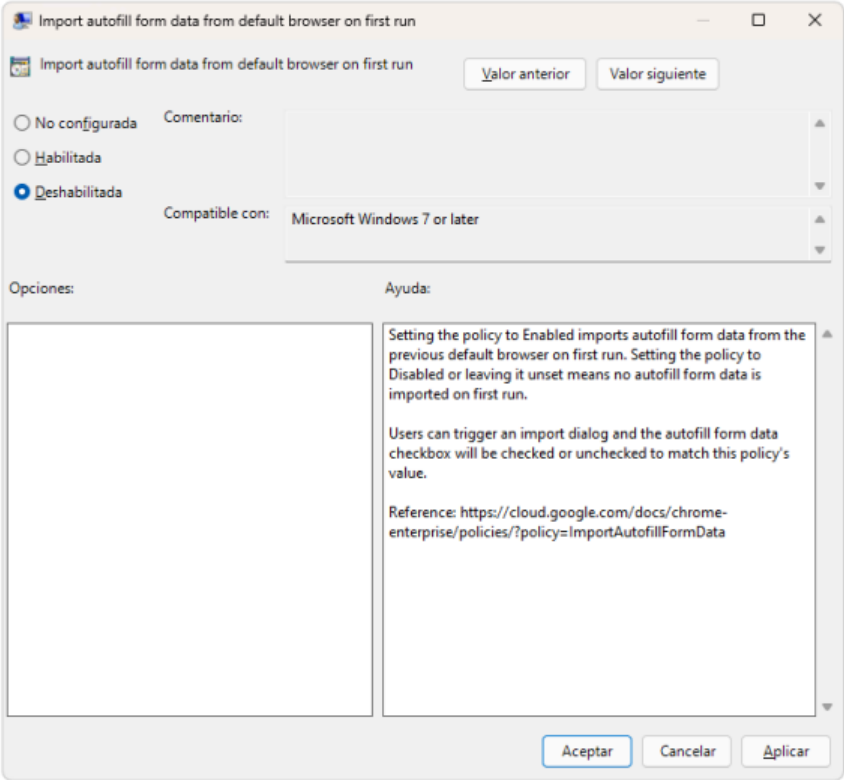
Impacto: Ninguno: este es el comportamiento predeterminado.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:ImportAutofillFormData
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Deshabilitada:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\Import autofill form data from default browser on first run
```



1.23 (L1) Ensure 'Import of homepage from default browser on first run' is set to 'Disabled' (Automated)

Descripción: esta configuración controla si los usuarios pueden importar la configuración de la página de inicio desde otro navegador a Google Chrome, así como si la configuración de la página de inicio se importa en el primer uso. Si establece esta configuración en Deshabilitado, los usuarios no podrán realizar una importación de la configuración de la página de inicio de otros navegadores a Google Chrome. El estado recomendado para esta configuración es: Deshabilitado (0)

Justificación: Tener la configuración de la página principal importada automáticamente o permitir que los usuarios importen esta configuración desde otro navegador a Google Chrome permite la posibilidad de que la configuración comprometida se importe a Google Chrome.

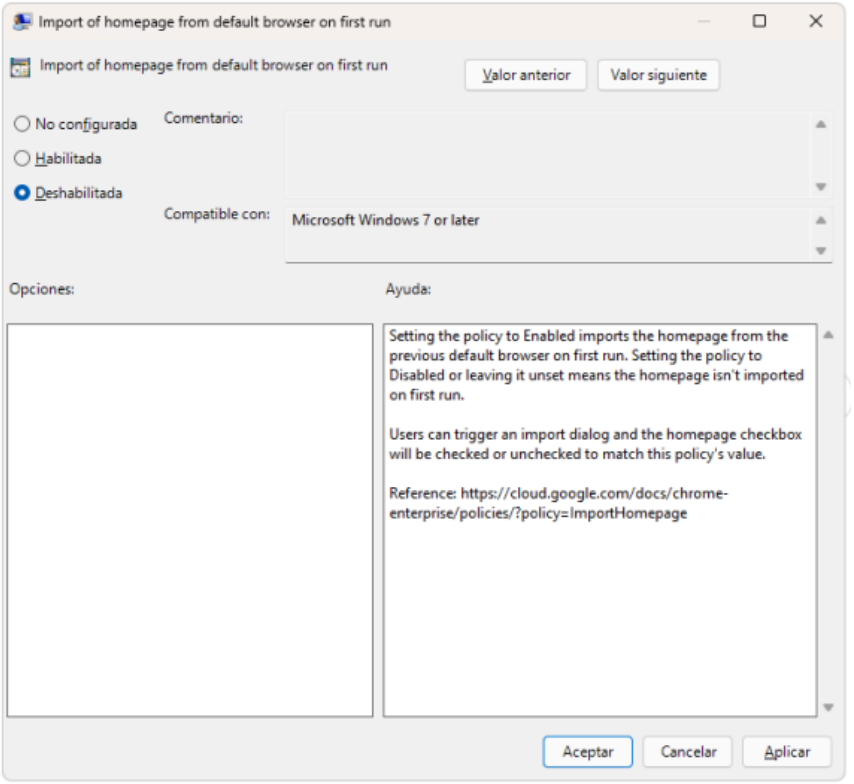
Impacto: Ninguno: este es el comportamiento predeterminado.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:ImportHomepage
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Deshabilitada:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\Import of homepage from default browser on first run
```



1.24 (L1) Ensure 'Import search engines from default browser on first run' is set to 'Disabled' (Automated)

Descripción: esta configuración controla si los usuarios pueden importar la configuración del motor de búsqueda desde otro navegador a Google Chrome, así como si dicha configuración se importa en el primer uso. Si establece esta configuración en Deshabilitado, los usuarios no podrán realizar una importación de la configuración de su motor de búsqueda desde otros navegadores a Google Chrome. El estado recomendado para esta configuración es: Deshabilitado (0)

Justificación: Importar automáticamente la configuración del motor de búsqueda o permitir que los usuarios importen la configuración de otro navegador a Google Chrome podría permitir que se establezca un motor de búsqueda malintencionado.

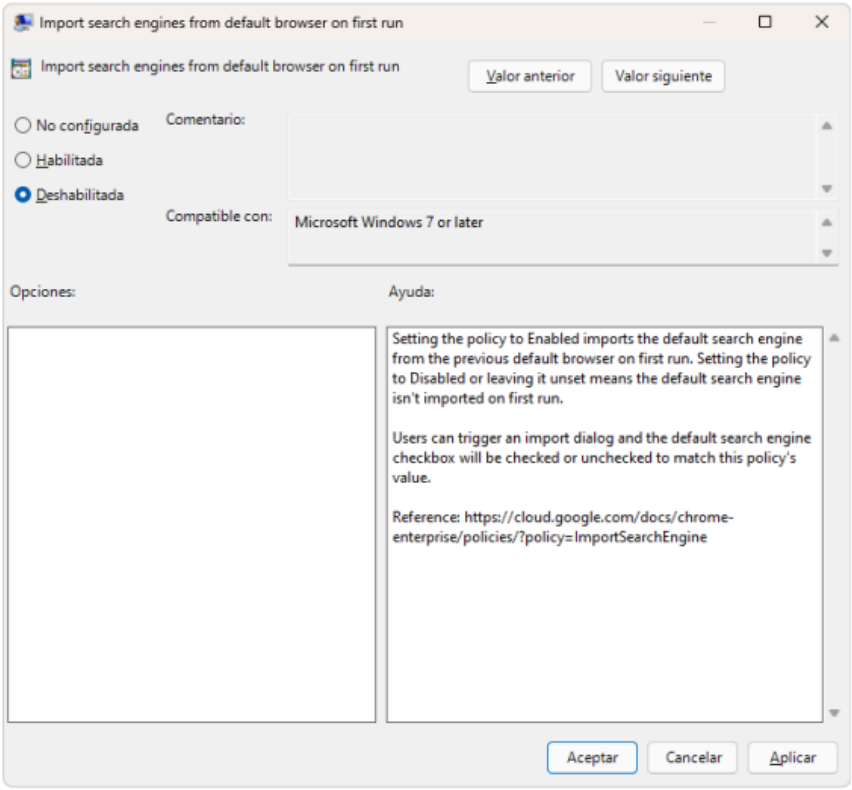
Impacto: Ninguno: este es el comportamiento predeterminado.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:ImportSearchEngine
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Deshabilitada:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\Import search engines from default browser on first run
```



1.25 (L1) Ensure 'List of names that will bypass the HSTS policy check' is set to 'Disabled' (Automated)

Descripción: esta configuración permite especificar una lista de nombres que estarán exentos de las comprobaciones de directiva HTTP Strict Transport Security

(HSTS) y, a continuación, se actualizarán potencialmente de http:// a https://. El estado recomendado para esta configuración es: Deshabilitado (0)

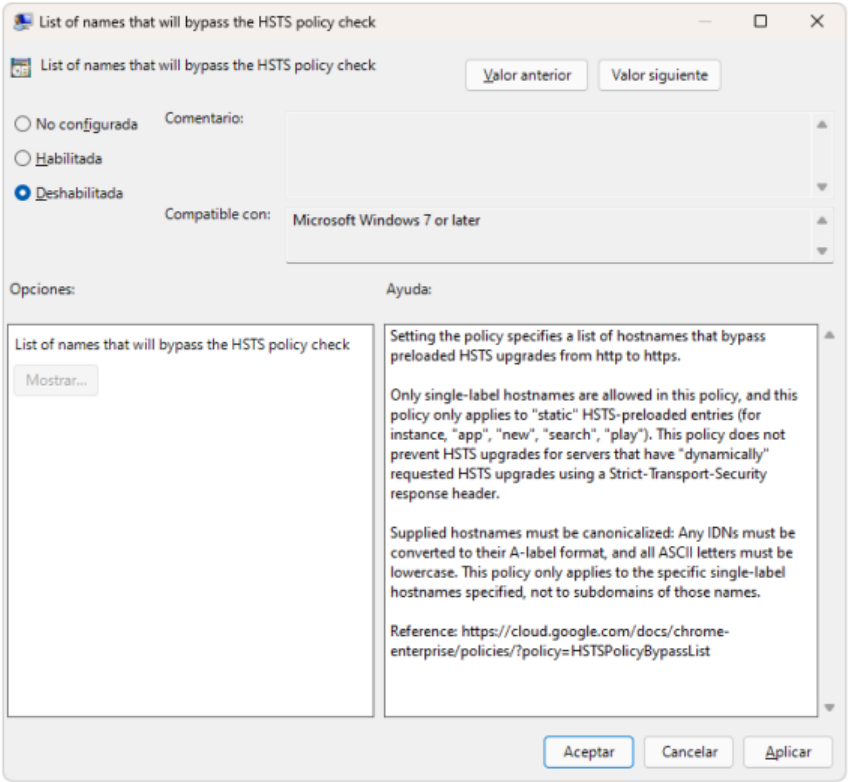
Justificación: Permitir que los nombres de host estén exentos de las comprobaciones de HSTS podría permitir ataques de degradación de protocolo y secuestros de cookies. Impacto: Ninguno: este es el comportamiento predeterminado.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta ruta de acceso del Registro no existirá si se establece en Deshabilitado:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\HSTSPolicyBypassList
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Deshabilitada:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\List of names that will bypass the HSTS policy check
```

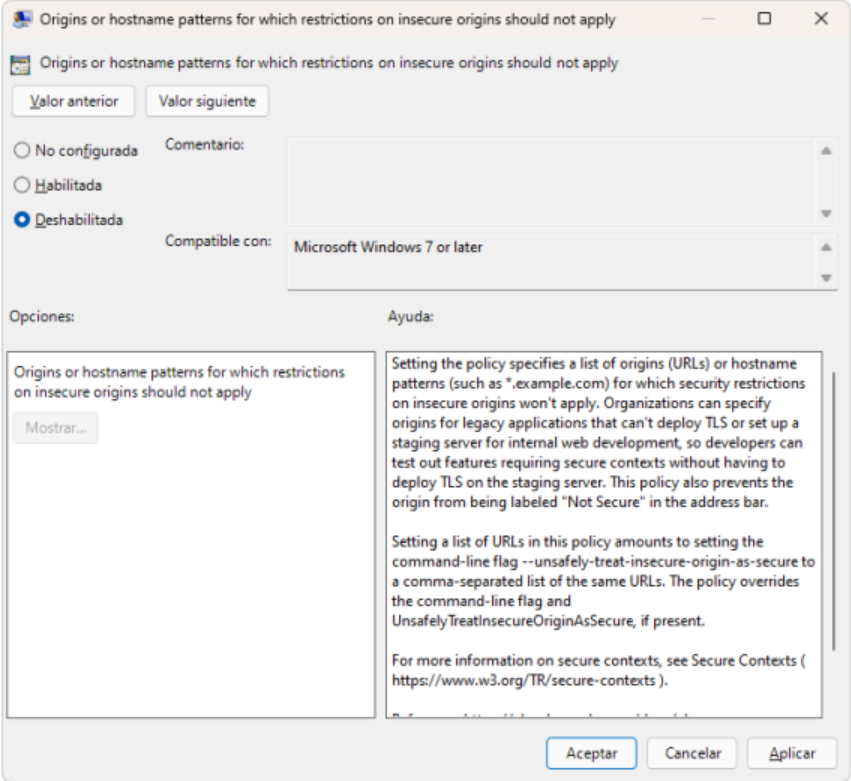


1.26 (L1) Ensure 'Origins or hostname patterns for which restrictions on insecure origins should not apply' is set to 'Disabled' (Automated)

Descripción: Google Chrome puede usar una lista de orígenes (URL) o patrones de nombres de host (por ejemplo, "*.example.com") a los que no se aplicarán restricciones de seguridad sobre orígenes no seguros y se evitará que se etiqueten como "No seguros" en el cuadro multifunción. El estado recomendado para esta configuración es: Deshabilitado (0)

Justificación: Los contextos inseguros siempre se etiquetarán como inseguros. Impacto: Ninguno: este es el comportamiento predeterminado.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta ruta de acceso del Registro no existirá si se establece en Deshabilitado:



1.27 (L1) Ensure 'Suppress lookalike domain warnings on domains' is set to 'Disabled' (Automated)

Descripción: esta configuración impide que se muestren advertencias de URL similares en los sitios enumerados. Por lo general, estas advertencias se muestran en sitios que Google Chrome cree que podrían estar intentando suplantar la identidad de otro sitio con el que el usuario está familiarizado.

• Deshabilitado (0) o establecido en una lista vacía: las advertencias pueden aparecer en cualquier sitio que visite el usuario.

• Habilitado (1) y configurado en uno o más dominios: no se mostrarán páginas de advertencia similares cuando el usuario visite páginas en ese dominio. El estado recomendado para esta configuración es: Deshabilitado (0)

Justificación: los dominios similares son engañosos intencionadamente para dar a los usuarios la falsa impresión de que están interactuando con marcas de confianza, lo que provoca un daño significativo a la reputación, pérdidas financieras y compromiso de datos para las empresas establecidas. Además, esta técnica se usa comúnmente para alojar sitios de phishing y, a menudo, conduce a ataques de apropiación de cuentas. A los usuarios se les pide que introduzcan sus credenciales en un sitio web falso, y los estafadores toman el control de sus cuentas en línea con poco esfuerzo para participar en actividades fraudulentas.

Impacto: Ninguno: este es el comportamiento predeterminado.

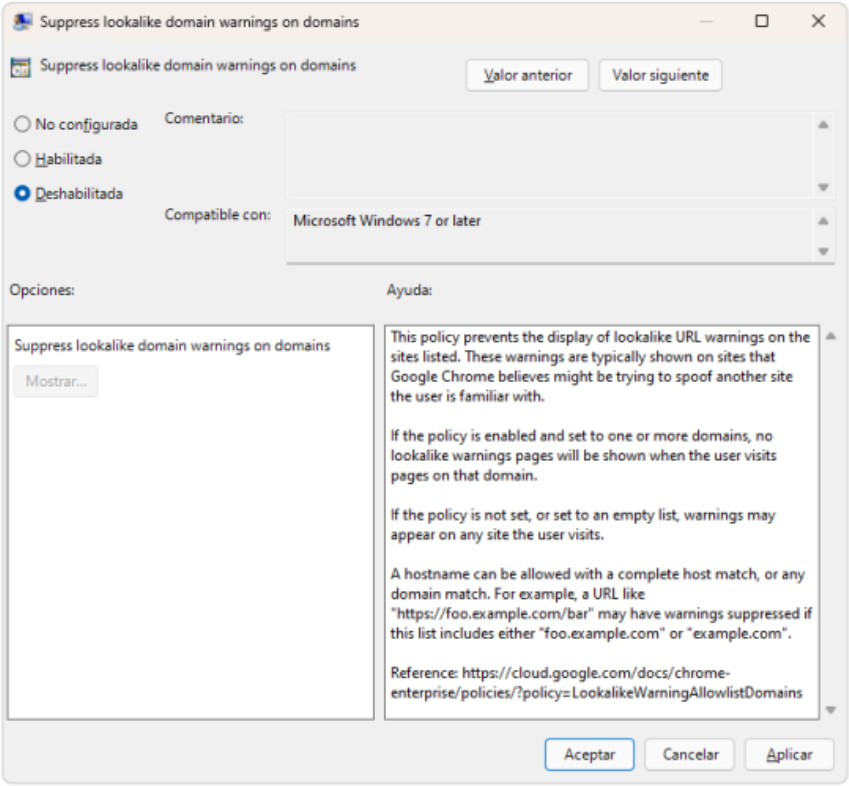
NOTA: El único impacto real es la posible molestia del usuario si va a un sitio legítimo que se considera falsamente fraudulento (una ocurrencia rara). Esto se puede manejar agregando el sitio a la lista de permitidos y/o notificando a Google sobre el hallazgo falso

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta ruta de acceso del Registro no existirá si se establece en Deshabilitado:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\LookalikeWarningAllowlistD
omains
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Deshabilitada:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\Suppress lookalike domain warnings on domains
```



1.28 (L1) Ensure 'Suppress the unsupported OS warning' is set to 'Disabled' (Automated)

Descripción: Google Chrome mostrará una advertencia cuando Google Chrome se esté ejecutando en un ordenador o sistema operativo que ya no sea compatible. El estado recomendado para esta configuración es: Deshabilitado (0) Justificación: Se informará al usuario si el software utilizado ya no es compatible.

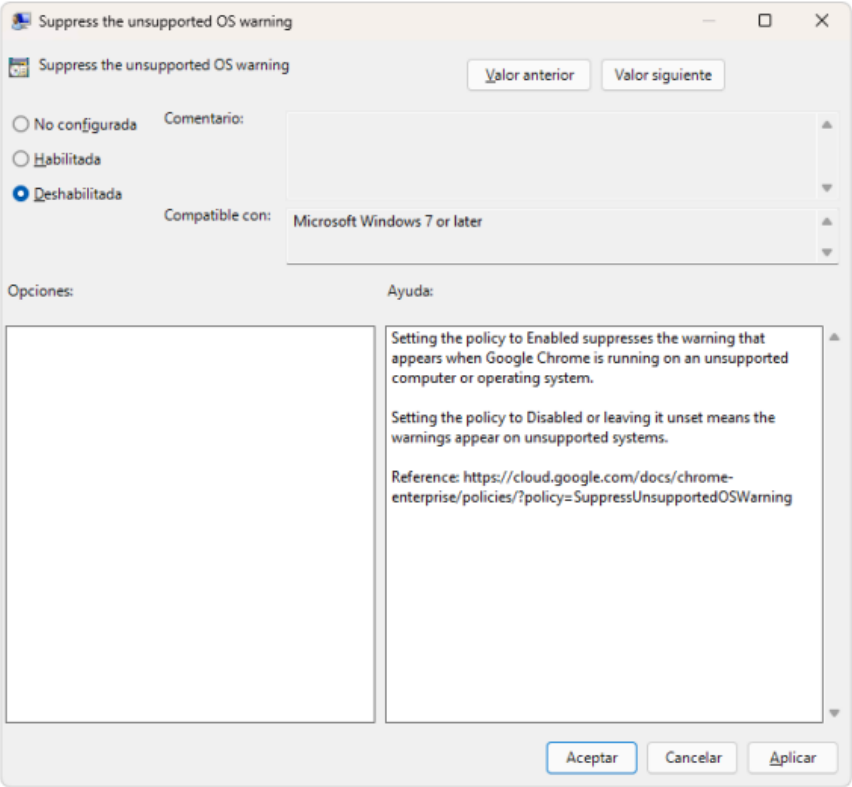
Impacto: Ninguno: este es el comportamiento predeterminado.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:SuppressUnsupportedOSWarni
ng
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Deshabilitada:

```
Computer Configuration\Polices\Administrative Templates\Google\Google
Chrome\Suppress the unsupported OS warning
```



1.29 (L1) Ensure 'URLs for which local IPs are exposed in WebRTC ICE candidates' is set to 'Disabled' (Automated)

Descripción: esta configuración especifica una lista de direcciones URL o patrones para los que WebRTC expondrá las direcciones IP locales. El estado recomendado para esta configuración es: Deshabilitado (0) NOTA: Esta configuración, si está habilitada, debilita la protección de las direcciones IP locales si los administradores lo necesitan.

Justificación: Habilitar esta configuración y permitir la exposición de direcciones IP puede permitir que un atacante recopile información sobre la red interna que podría utilizarse para violar y atravesar una red.

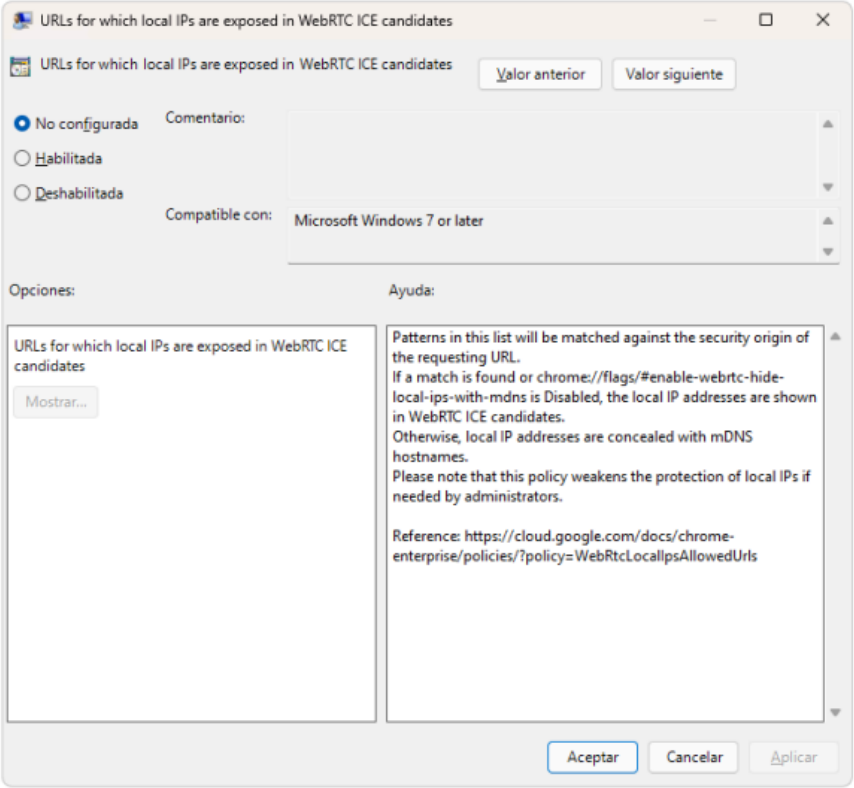
Impacto: Ninguno: este es el comportamiento predeterminado.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo no tendrá ningún valor del Registro (la clave no existirá) si se establece en Deshabilitado:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\WebRtcLocalIpsAllowedUrls
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Deshabilitada:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\URLs for which local IPs are exposed in WebRTC ICE candidates
```



2 Attack Surface Reduction

Esta sección contiene recomendaciones que ayudan a reducir la superficie de ataque general. Las organizaciones deben revisar esta configuración y los posibles impactos para asegurarse de que tengan sentido dentro del entorno, ya que restringen algunas funciones del explorador

2.1 Update settings (Google section of GPO)

Esta configuración no se encuentra en la sección normal GoogleGoogle Chrome del GPO

2.1.1 (L1) Ensure 'Update policy override' is set to 'Enabled' with 'Always allow updates (recommended)' or 'Automatic silent updates' specified (Automated)

Descripción: Google Update gestiona la instalación de las actualizaciones de Google Chrome disponibles de Google. Esta configuración permite a los usuarios definir si las actualizaciones se aplicarán automáticamente. Dependiendo del escenario empresarial, las actualizaciones se aplicarán periódicamente o también si el usuario busca actualizaciones.

- Actualizaciones deshabilitadas: Nunca aplicar actualizaciones (0)
- Permitir siempre actualizaciones: las actualizaciones siempre se aplican cuando se encuentran, ya sea mediante una comprobación periódica de actualizaciones o mediante una comprobación manual de actualizaciones (1)
- Solo actualizaciones manuales: las actualizaciones solo se aplican cuando el usuario realiza una comprobación de actualización manual (2)
- Solo actualizaciones automáticas silenciosas: las actualizaciones solo se aplican cuando se encuentran a través de la comprobación periódica de actualizaciones (3)

Desactivado (0): Google Update gestiona las actualizaciones disponibles según lo especificado en "Anulación predeterminada de la política de actualizaciones".

El estado recomendado para esta configuración es: Habilitado con un valor de Permitir siempre actualizaciones (1) o Actualizaciones silenciosas automáticas (3)

NOTA: Esta directiva solo está disponible en instancias de Windows que están unidas a un dominio de Microsoft® Active Directory®.

Justificación: Las actualizaciones de software se aplicarán tan pronto como estén disponibles, ya que pueden incluir los últimos parches de seguridad.

Impacto: Las actualizaciones más recientes se aplican automáticamente al menos periódicamente.

Auditoría: Navegue hasta la ruta de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 1 o 3:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Update:Update{8A69D345-D564-463C-
AFF1-A69D9E530F96}
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Habilitada: Permitir siempre actualizaciones (recomendado):

```
Computer Configuration\Polices\Administrative Templates\Google\Google
Update\Applications\Google Chrome\Update policy override
```

2.2 Content settings

2.2.1 (L1) Ensure 'Control use of insecure content exceptions' is set to 'Enabled: Do not allow any site to load mixed content' (Automated)

Descripción: la configuración controla si los usuarios pueden agregar excepciones para permitir contenido mixto para sitios específicos.

- No permitir que ningún sitio cargue contenido mixto (2)
- Permitir que los usuarios agreguen excepciones para permitir contenido mixto (3)

El estado recomendado para esta configuración es: Habilitado con el valor de No permitir que ningún sitio cargue contenido mixto (2)

NOTA: Esta directiva se puede invalidar para patrones de URL específicos mediante las directivas Insecure Content Allowed For Urls e Insecure Content Blocked For Urls.

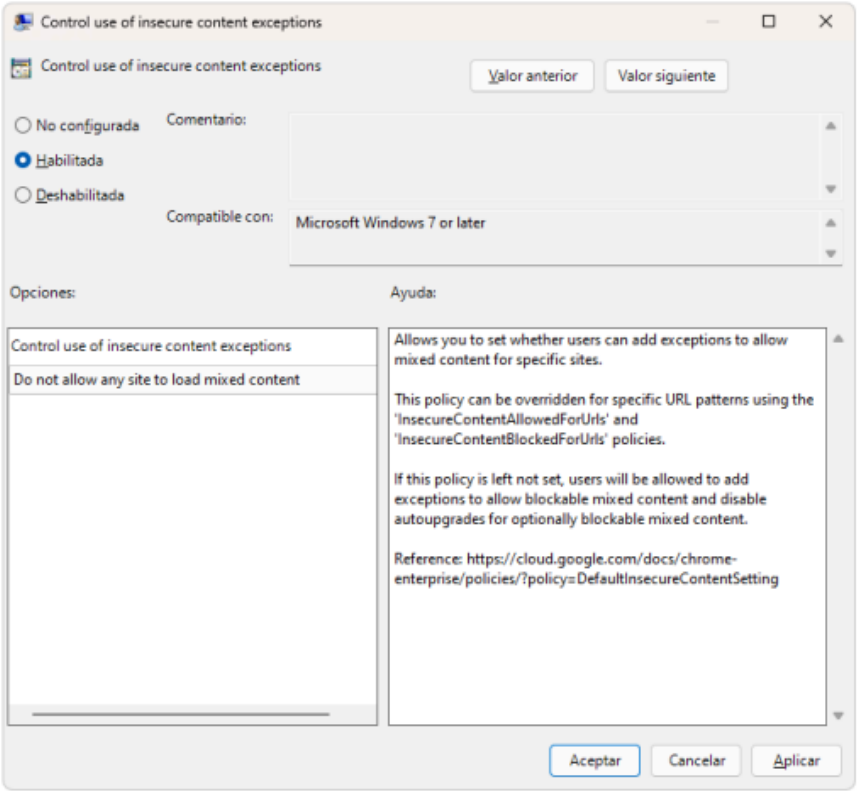
Justificación: Permitir contenido mixto (seguro / inseguro) de un sitio puede provocar la carga de contenido malicioso. El contenido mixto se produce si la solicitud inicial es segura a través de HTTPS, pero el contenido HTTPS y HTTP se carga posteriormente para mostrar la página web. El contenido HTTPS es seguro. El contenido HTTP no es seguro.

Impacto: los usuarios no podrán mezclar contenido. Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 2:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:DefaultInsecureContentSett
ing
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Habilitada: No permita que ningún sitio cargue contenido mixto:

```
Computer Configuration\Polices\Administrative Templates\Google\Google
Chrome\Content Settings\Control use of insecure content exceptions
```



2.2.2 (L2) Ensure 'Control use of the Web Bluetooth API' is set to 'Enabled: Do not allow any site to request access to Bluetooth devices via the Web Bluetooth API' (Automated)

Descripción: Google Chrome tiene una API que permite el acceso a dispositivos Bluetooth cercanos desde el navegador con el consentimiento de los usuarios.

• No permita que ningún sitio solicite acceso a dispositivos Bluetooth a través de la API de Web Bluetooth (2)

• Permitir que los sitios pidan al usuario que conceda acceso a un dispositivo Bluetooth cercano (3)

El estado recomendado para esta configuración es: Habilitado con un valor de No permitir que ningún sitio solicite acceso a dispositivos Bluetooth a través de la API de Web Bluetooth (2)

Justificación: Un sitio web malicioso podría explotar un dispositivo Bluetooth vulnerable.

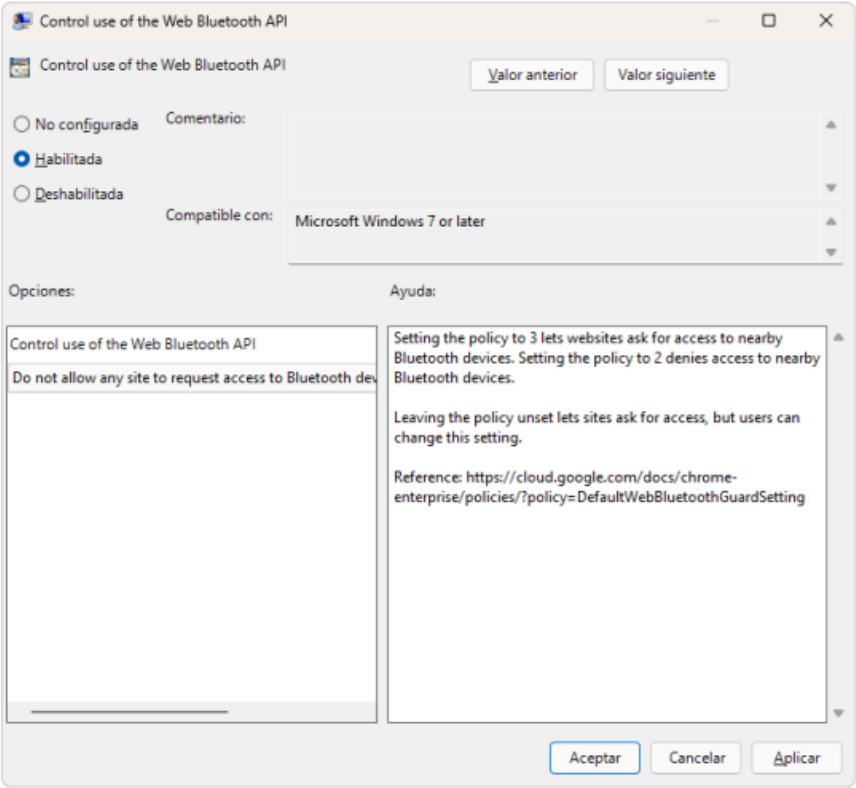
Impacto: Si se configura esta opción, los sitios web ya no podrán acceder a dispositivos Bluetooth cercanos a través de la API (esto incluye cámaras web, auriculares y otros dispositivos Bluetooth) y nunca se le preguntará al usuario.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 2:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:DefaultWebBluetoothGuardSe
tting
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Habilitada: No permita que ningún sitio solicite acceso a dispositivos Bluetooth a través de la API de Bluetooth web:

```
Computer Configuration\Polices\Administrative Templates\Google\Google
Chrome\Content Settings\Control use of the Web Bluetooth API
```



2.2.3 (L2) Ensure 'Control use of the WebUSB API' is set to 'Enabled: Do not allow any site to request access to USB devices via the WebUSB API' (Automated)

Descripción: Google Chrome tiene una API que permite el acceso a los dispositivos USB conectados desde el navegador

• No permita que ningún sitio solicite acceso a dispositivos USB a través de la API WebUSB (2)

• Permitir que los sitios soliciten al usuario que otorgue acceso a un dispositivo USB conectado (3)

El estado recomendado para esta configuración es: Habilitado con un valor de No permitir que ningún sitio solicite acceso a dispositivos USB a través de la API WebUSB (2) Justificación: WebUSB está abriendo las puertas a sofisticados ataques de phishing que podrían eludir los dispositivos de autenticación de dos factores basados en hardware (por ejemplo, los dispositivos Yubikey).

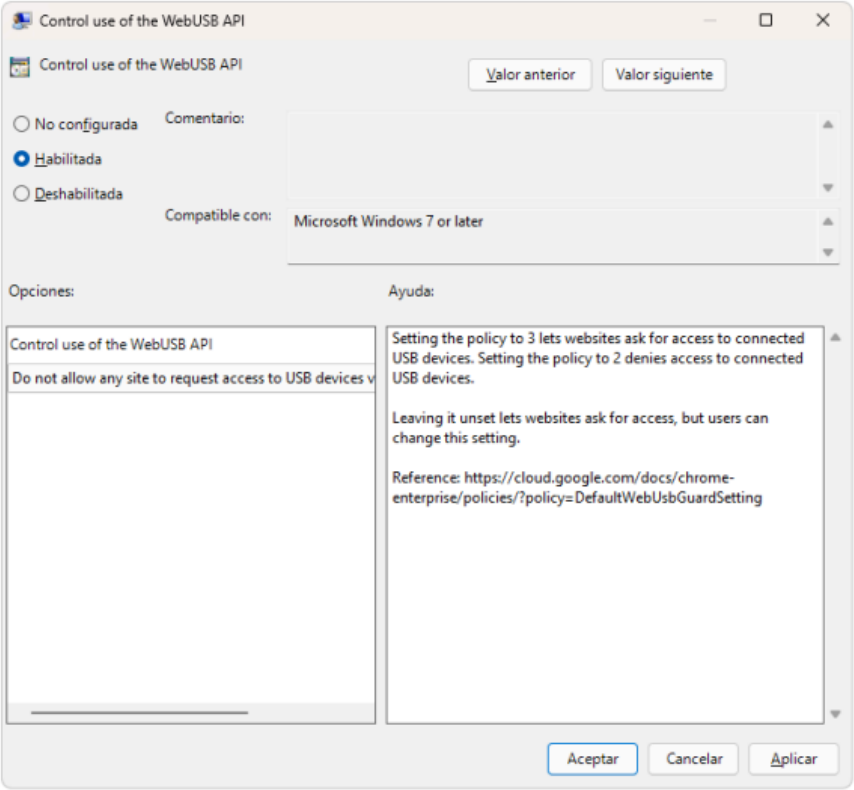
Impacto: Si se configura esta opción, los sitios web ya no pueden acceder a los dispositivos USB conectados a través de la API (esto incluye cámaras web, auriculares y otros dispositivos USB), lo que también podría impedir que algunos dispositivos USB de autenticación de dos factores (2FA) funcionen correctamente.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 2:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:DefaultWebUsbGuardSetting
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Habilitada: No permita que ningún sitio solicite acceso a dispositivos USB a través de la API de WebUSB:

```
Computer Configuration\Polices\Administrative Templates\Google\Google
Chrome\Content Settings\Control use of the WebUSB API
```



2.2.4 (L2) Ensure 'Default notification setting' is set to 'Enabled: Do not allow any site to show desktop notifications' (Automated)

Descripción: Google Chrome tiene una API que permite el acceso a los dispositivos USB conectados desde el navegador

- No permita que ningún sitio solicite acceso a dispositivos USB a través de la API WebUSB (2)
- Permitir que los sitios soliciten al usuario que otorgue acceso a un dispositivo USB conectado (3)

El estado recomendado para esta configuración es: Habilitado con un valor de No permitir que ningún sitio solicite acceso a dispositivos USB a través de la API WebUSB (2)

Justificación: WebUSB está abriendo las puertas a sofisticados ataques de phishing que podrían eludir los dispositivos de autenticación de dos factores basados en hardware (por ejemplo, los dispositivos Yubikey).

Impacto: Si se configura esta opción, los sitios web ya no pueden acceder a los dispositivos USB conectados a través de la API (esto incluye cámaras web, auriculares y

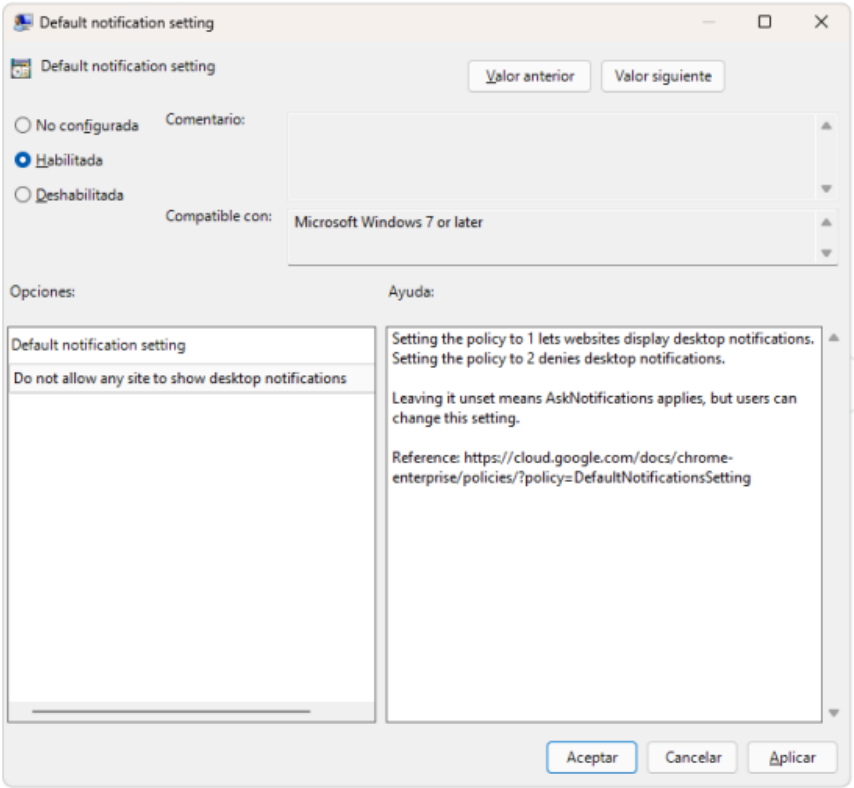
otros dispositivos USB), lo que también podría impedir que algunos dispositivos USB de autenticación de dos factores (2FA) funcionen correctamente.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 2:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:DefaultNotificationsSettin
g
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Habilitada: No permita que ningún sitio muestre notificaciones de escritorio:

```
Computer Configuration\Polices\Administrative Templates\Google\Google
Chrome\Content Settings\Default notification setting
```



2.2.5 (L1) Ensure 'Allow local file access to file:// URLs on these sites in the PDF Viewer' Is Disabled (Automated)

Descripción: esta configuración permitirá que las URL especificadas accedan a file:// URL en el visor de PDF. De forma predeterminada, se bloquea el acceso de todos los dominios a file:// URL en el visor de PDF

Justificación: Bloquear todos los dominios, o una lista restringida de dominios, para que no abran un archivo PDF descargado bloquea la posibilidad de que un archivo malintencionado se enmascare como PDF. También podría bloquear el código desconocido o malicioso contenido en el PDF que se ejecutaría al abrirse inmediatamente dentro de una pestaña del navegador.

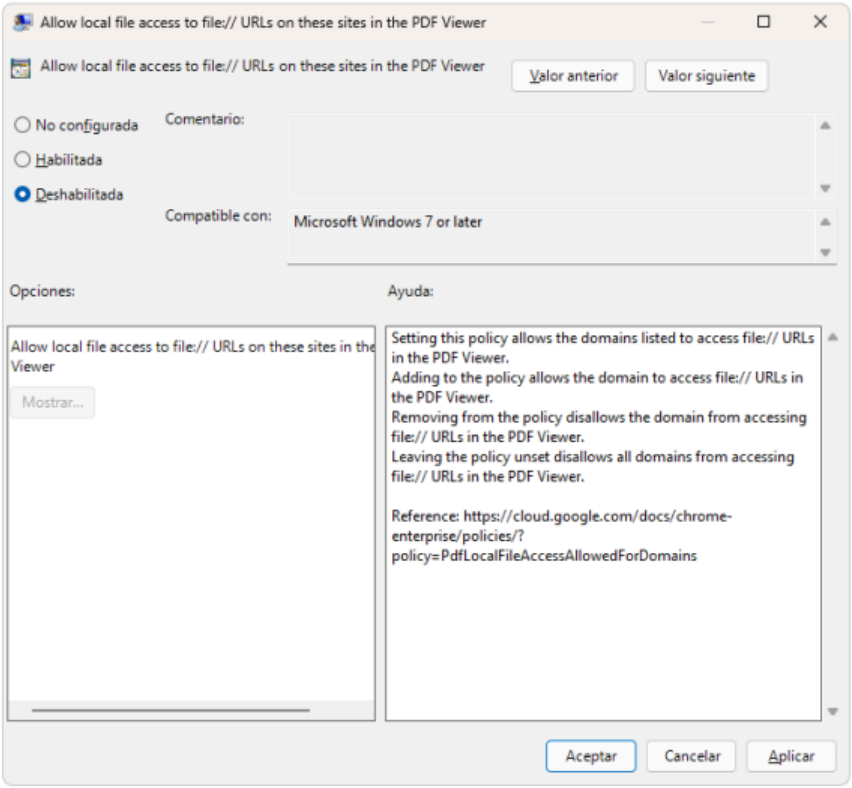
Impacto: Los usuarios deberán abrir los archivos PDF manualmente en el visor de PDF o en la aplicación de visualización de PDF de la organización.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo no tendrá ningún valor del Registro (la clave no existirá) si se establece en Deshabilitado:

```
HKEY LOCAL MACHINE\SOFTWARE\Policies\Google\Chrome\PdfLocalFileAccessAllowedF
orDomains\
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Deshabilitada:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\Content settings\Allow local file access to file:// URLs on these
sites in the PDF Viewer
```



2.3 Extensions

2.3.1 (L1) Ensure 'Blocks external extensions from being installed' is set to 'Enabled' (Automated)

Descripción: Al habilitar esta opción, se bloquea la instalación de extensiones externas (una extensión que no está instalada desde Chrome Web Store). El estado recomendado para esta configuración es: Habilitado (1)

Justificación: Permitir que los usuarios instalen extensiones desde otras ubicaciones (no desde Chrome Web Store) puede provocar la instalación de extensiones maliciosas.

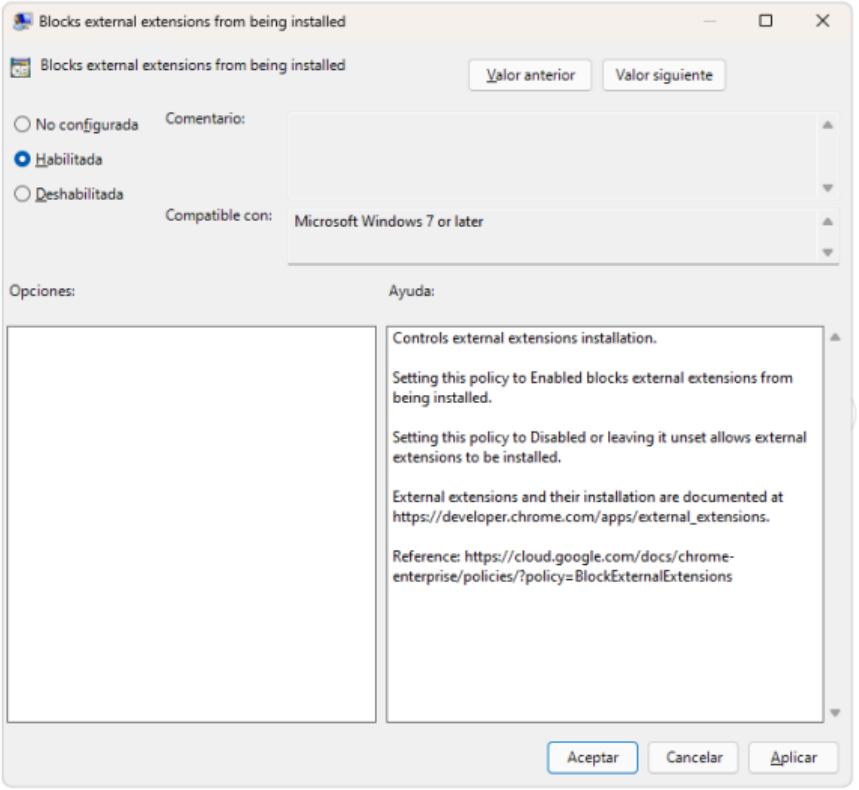
Impacto: El usuario solo podrá instalar la extensión para Chrome Web Store.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 1:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:BlockExternalExtensions
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Habilitada:

```
Computer Configuration\Polices\Administrative Templates\Google\Google
Chrome\Extensions\Blocks external extensions from being installed
```



2.3.2 (L1) Ensure 'Configure allowed app/extension types' is set to 'Enabled: extension, hosted_app, platform_app, theme' (Automated)

Descripción: al habilitar esta configuración, puede especificar qué tipos de aplicaciones o extensiones se permiten. Deshabilitado (0): no da como resultado restricciones en los tipos de extensión y aplicación aceptables. El estado recomendado para esta configuración es: Habilitado con los valores de extensión, hosted_app, platform_app, tema.

Justificación: Los tipos de aplicaciones o extensiones que podrían usarse incorrectamente o que están en desuso ya no se instalarán.

NOTA: Google ha eliminado la compatibilidad con las aplicaciones de Chrome, que incluye los tipos hosted_app y platform_app. La publicación del blog indica que estos

tipos requerirán que se habilite una configuración para su uso continuo hasta junio de 2022.

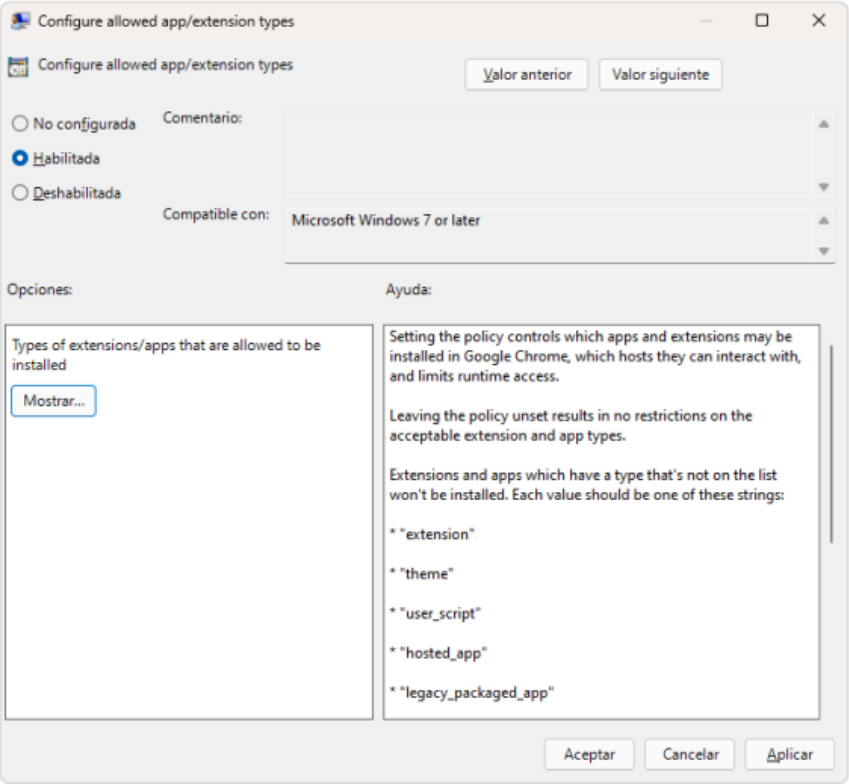
Impacto: Las extensiones ya instaladas se eliminarán si su tipo está en la lista de bloqueados y la extensión en sí no está incluida en la lista de permitidos.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro que debe establecerse en extension, hosted_app, platform_app, theme:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\ExtensionAllowedTypes:
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Habilitado: extensión, hosted_app, platform_app, tema:

```
Computer Configuration\Polices\Administrative Templates\Google\Google
Chrome\Extensions\Configure allowed app/extension types
```



2.3.3 (L1) Ensure 'Configure extension installation blocklist' is set to 'Enabled: *' (Automated)

Descripción: Habilitar esta configuración le permite especificar qué extensiones NO pueden instalar los usuarios. Las extensiones ya instaladas se eliminarán si están en la lista de bloqueo. Deshabilitado (0): entonces el usuario puede instalar cualquier extensión en Google Chrome. El estado recomendado para esta configuración es: Habilitado con un valor de *

NOTA: Chrome ofrece una configuración más detallada basada en permisos llamada Configuración de administración de extensiones si la lista de bloqueo de todas las extensiones es demasiado agresiva, lo que permite a una organización explorar en profundidad los permisos exactos que desea bloquear. La configuración de administración de extensiones requiere más coordinación y esfuerzo para comprender cuáles son los requisitos de seguridad para bloquear los permisos de sitios y dispositivos globalmente, así como más administración de TI para implementar. El beneficio sería permitir el acceso a más extensiones a sus usuarios finales.

NOTA: Si Chrome Cleanup está inhabilitado, es posible que los usuarios deseen configurar la lista de bloqueo de extensiones en lugar de usar la opción Administración de extensiones. La limpieza de Chrome puede ayudar a proteger contra extensiones maliciosas cuando se combina con la configuración de Administración de extensiones.

Justificación: Esto se puede utilizar para bloquear extensiones que podrían permitir el control remoto del sistema a través del navegador. Si se necesitan extensiones para proteger el explorador o para uso empresarial, se pueden habilitar configurando la opción Configurar lista de permitidos de instalación de extensiones o la configuración Configuración de administración de extensiones.

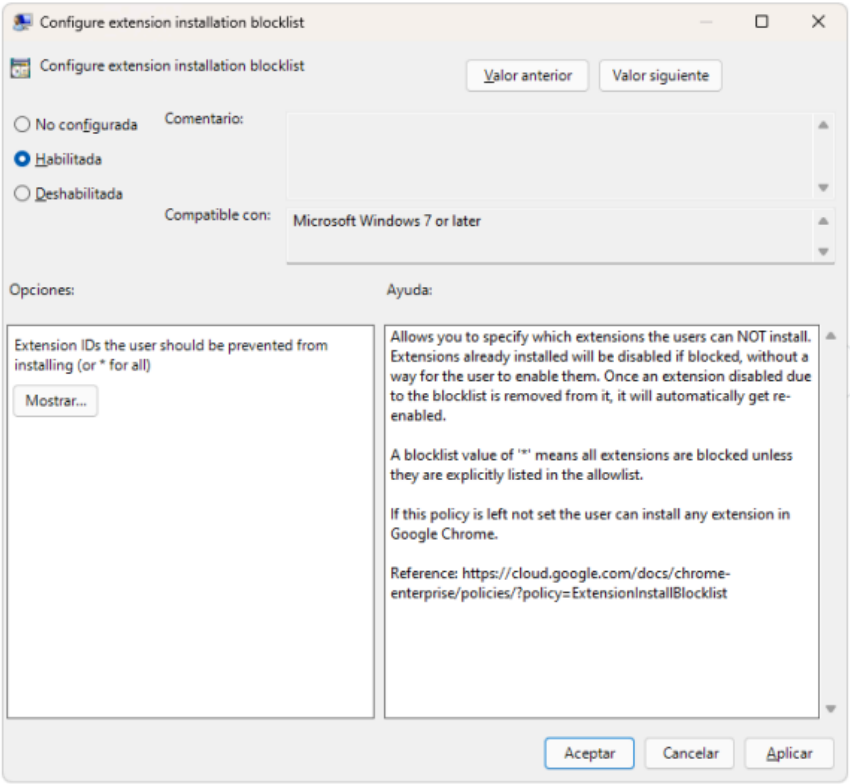
Impacto: se quitará cualquier extensión instalada a menos que se especifique en la lista de extensiones permitidas. Si una organización utiliza algún administrador de contraseñas aprobado, asegúrese de que la extensión se agregue a la lista de permitidos

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en *:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\ExtensionInstallBlocklist:
1
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Habilitado y un valor de * para los identificadores de extensión que el usuario debe no poder instalar:

```
Computer Configuration\Polices\Administrative Templates\Google\Google
Chrome\Extensions\Configure extension installation blocklist
```



2.3.4 (L2) Ensure 'Default third-party storage partitioning setting' Is Enabled and Blocked (Automated)

Descripción: esta configuración bloqueará el acceso de cualquier sitio a la sesión de almacenamiento desde cualquier otro sitio. Esto impedirá que los rastreadores de terceros que están incrustados en varios sitios rastreen a un usuario en los sitios que visitan. Bloquear el acceso de terceros al agente de usuario no permitirá que los sitios infieran datos sobre el usuario a partir de los datos de otro sitio. Se puede configurar para:

- Habilitado (1): Permitir que se habilite la creación de particiones de almacenamiento de terceros.
- Deshabilitado (2): bloquea la habilitación de particiones de almacenamiento de terceros.

Justificación: Para establecer esto, es necesario que el estado del agente de usuario tenga más de un origen o sitio codificado. También puede defenderse contra los ataques de sincronización en la privacidad web. Impacto: la aplicación de esta medida puede

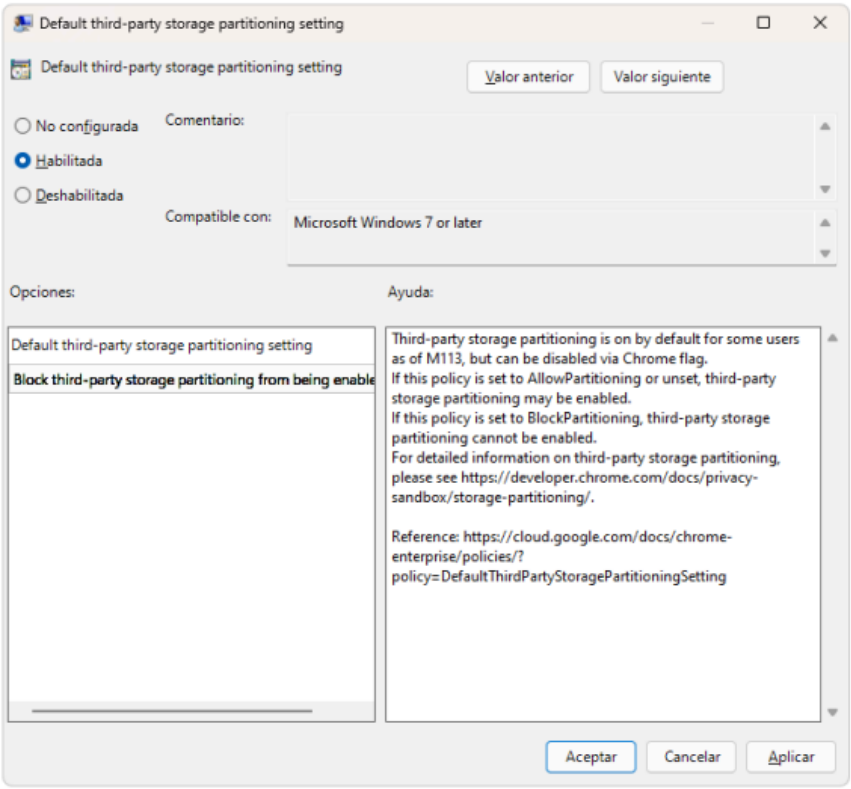
provocar que los usuarios experimenten problemas con los sitios que visitan con regularidad y que ya conceden acceso a terceros.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse individualmente en las direcciones URL permitidas de la organización:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\DefaultThirdPartyStoragePa
rtitioningSetting:2
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Habilitado: Bloquear la creación de particiones de almacenamiento de terceros para que no se habilite.:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\Content settings\Default third-party storage partitioning setting
```



2.3.5 (L1) Ensure 'Block third-party storage partitioning for these origins' Is Configured (Manual)

Descripción: esta configuración bloqueará los sitios específicos que seleccione su organización para que no accedan a la sesión de almacenamiento desde cualquier otro sitio. Esto permitirá a una organización bloquear los rastreadores de terceros que están incrustados en varios sitios para que no rastreen a un usuario en los sitios que visita. También permitirá bloquear el acceso de terceros al agente de usuario e inferir datos sobre el usuario a partir de los datos de otro sitio. Al establecer la recomendación de nivel 2 DefaultThirdPartyStoragePartitioningSetting, se bloquearán todos los sitios, no solo esta lista establecida en ThirdPartyStoragePartitioningBlockedForOrigins Justificación: Si su organización no desea bloquear el acceso de todos los sitios de terceros al agente de usuario, puede configurar una lista seleccionada de sitios para bloquear.

Impacto: esto puede hacer que la experiencia del usuario varíe de sitios permitidos a sitios bloqueados.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse individualmente en las direcciones URL permitidas de la organización:

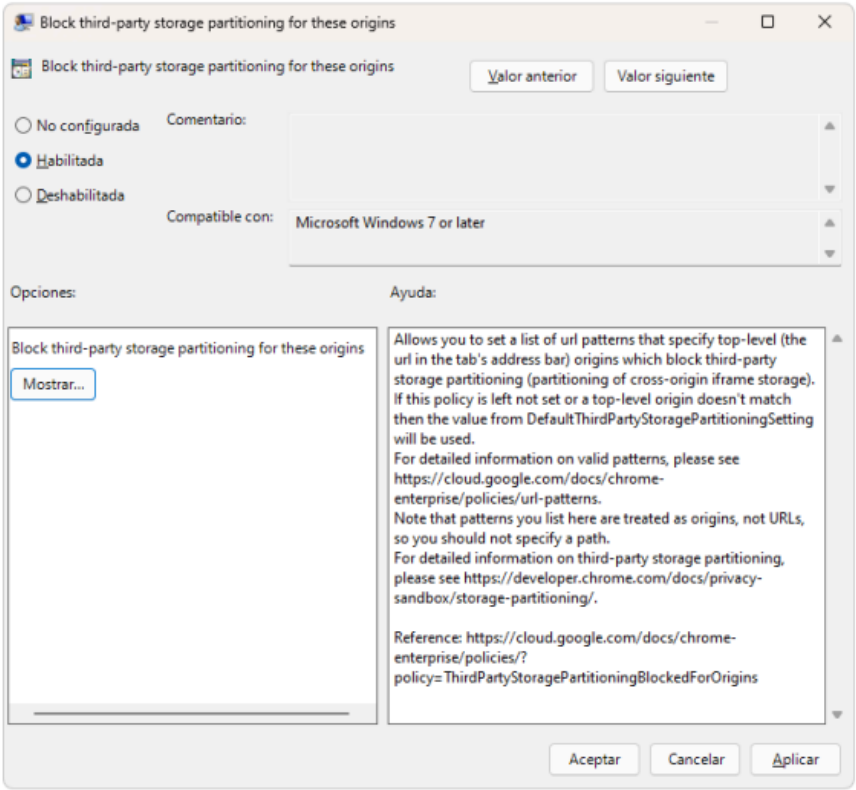
```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\ThirdPartyStoragePartition
ingBlockedForOrigins\<number> = <url>
```

Ejemplo:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\ThirdPartyStoragePartition
ingBlockedForOrigins\1 = https://www.example.com
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\ThirdPartyStoragePartition
ingBlockedForOrigins\2 = [*.]example.edu
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\ThirdPartyStoragePartition
ingBlockedForOrigins\3 = https://www.example.net
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Habilitada y establezca Mostrar en las direcciones URL aprobadas:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\Content settings\Block third-party storage partitioning for these
origins
```



2.3.6 (L2) Ensure 'Control Manifest v2 extension availability' Is Set to Forced Only (Automated)

Descripción: esta configuración de directiva controla la configuración de administración de extensiones para Google Chrome, específicamente las extensiones v2. Esta configuración de política se está eliminando a medida que Google desarrolla el Manifiesto v3, pero ese lanzamiento se pospone actualmente. La directiva se puede configurar para:

- Predeterminado (0): Comportamiento predeterminado del explorador
- Deshabilitado (1): El manifiesto v2 está deshabilitado
- Habilitado (2): El manifiesto v2 está habilitado
- Solo forzado (3): El manifiesto v2 está habilitado solo para extensiones forzadas

Justificación: Establecer esto en Solo forzado no permitirá a los usuarios instalar ninguna extensión v2 adicional y se deshabilitarán todas las extensiones v2 existentes y no forzadas.

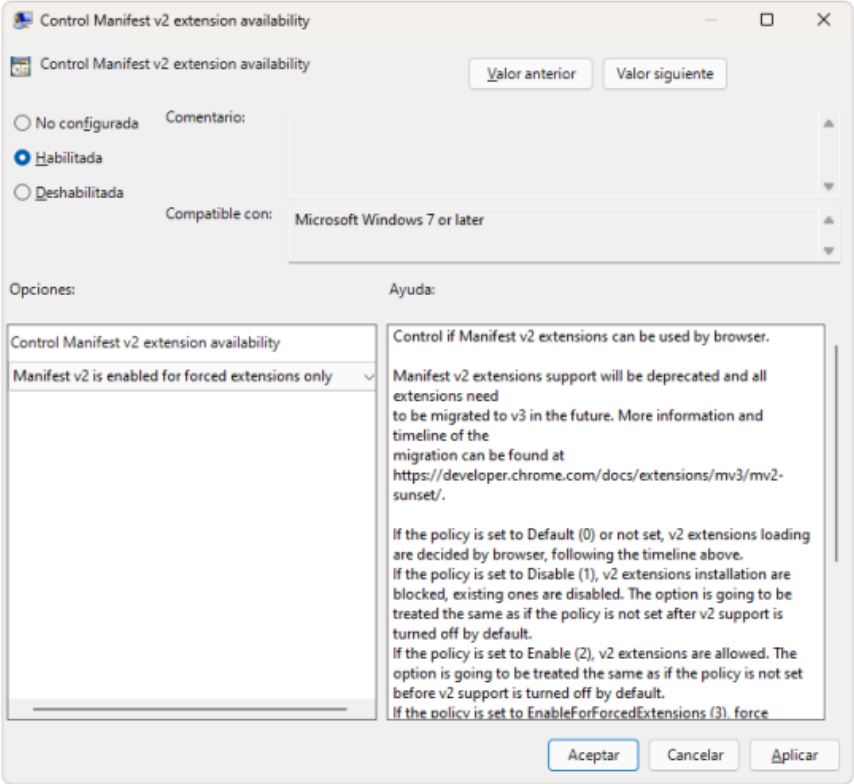
Impacto: los usuarios que usan extensiones con regularidad tendrán un conjunto de ellas bloqueado, lo que cambiará su experiencia de usuario.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 3:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:ExtensionManifestV2Availab
ility
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Habilitado: El manifiesto v2 solo está habilitado para extensiones forzadas:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\Extensions\Control Manifest v2 extension availability
```



2.3.7 (L1) Ensure 'Control availability of extensions unpublished on the Chrome Web Store' Is Disabled (Automated)

Descripción: esta política inhabilita todas las extensiones de Google Chrome que se descargaron de Chrome Web Store y que ahora no se han publicado. La directiva se puede configurar para:

• Habilitado (0): Permitir extensiones no publicadas

• Deshabilitado (1): Deshabilitar extensiones no publicadas Si el valor de ExtensionUnpublishedAvailability no se cambia con respecto al valor predeterminado, se comportará como está habilitado.

Nota: Se ignoran las extensiones fuera de la tienda, como las extensiones desempaquetadas instaladas con el modo de desarrollador y las extensiones instaladas con el modificador de línea de comandos. Se omiten las extensiones instaladas por fuerza que son autohospedadas. También se omiten todas las extensiones ancladas a la versión.

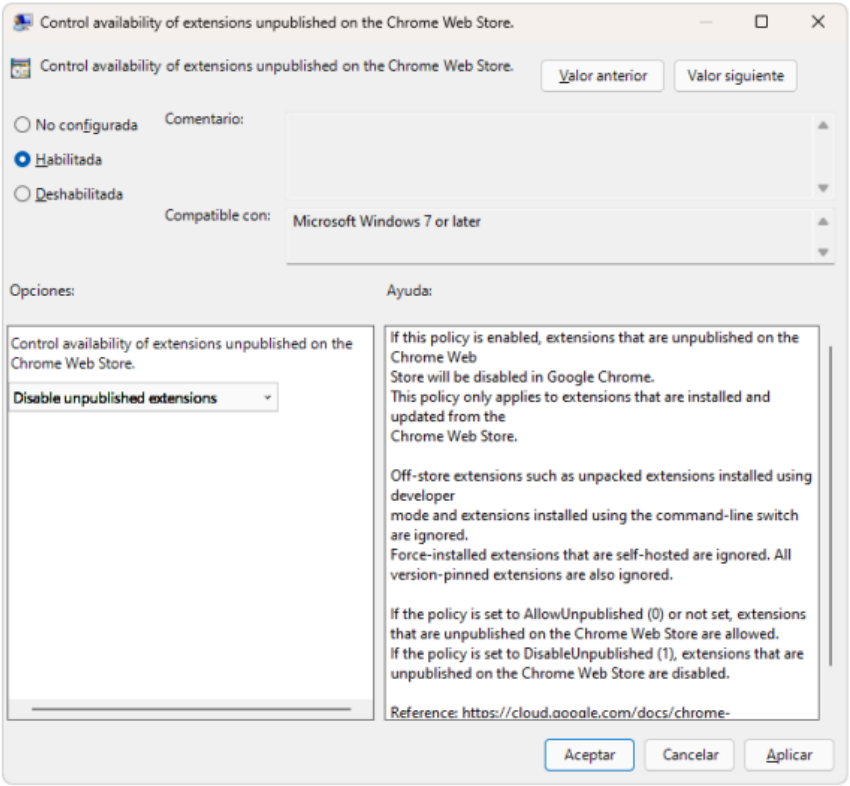
Justificación: Al deshabilitar las extensiones no publicadas, se eliminará la capacidad de ejecutar las extensiones que ya no se actualizan o revisan. Impacto: esto puede deshabilitar las extensiones que suelen usar los usuarios de su organización.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 1:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:ExtensionUnpublishedAvaila
bility
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Habilitada: Deshabilite las extensiones no publicadas:

```
Computer Configuration\Policies\Administrative Templates\Google
Chrome\Extensions\Control availability of extensions unpublished on the
Chrome Web Store.
```



2.4 HTTP AUTHENTICATION

2.4.1 (L2) ENSURE 'SUPPORTED AUTHENTICATION SCHEMES' IS SET TO 'ENABLED: NTLM, NEGOTIATE' (AUTOMATED)

Descripción: especifica qué esquemas de autenticación HTTP son compatibles con Google Chrome. Deshabilitado (0): Permite todos los esquemas de autenticación compatibles. El estado recomendado para esta configuración es: Habilitado con el valor de ntlm, negotiate

Justificación: Los valores posibles son 'basic', 'digest', 'ntlm' y 'negotiate'. La autenticación básica y implícita no proporcionan suficiente seguridad y pueden dar lugar al envío de contraseñas de usuario en texto no cifrado o con una protección mínima (la autenticación integrada solo se admite para los desafíos de negociación y ntlm).

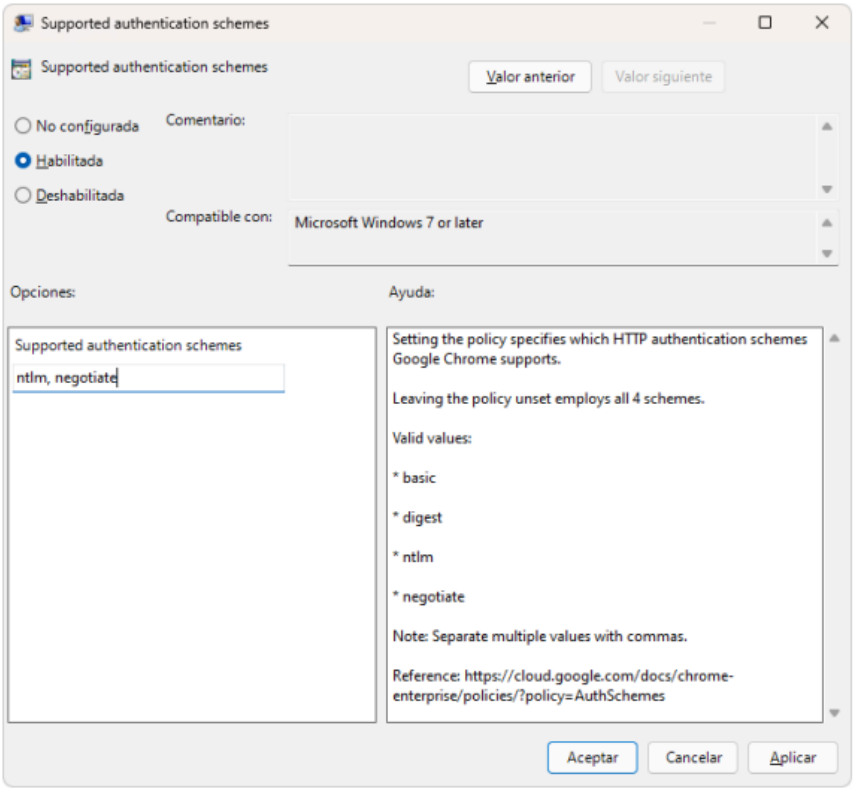
Impacto: Si algunas aplicaciones o sitios web heredados requerían mecanismos de autenticación inseguros, no funcionarían correctamente.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro que debe establecerse en ntlm, negotiate:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:AuthSchemes
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Habilitado: ntlm, negotiate:

```
Computer Configuration\Polices\Administrative Templates\Google\Google
Chrome\HTTP Authentication\Supported authentication schemes
```



2.5 Native Messaging

2.5.1 (L2) Ensure 'Configure native messaging blocklist' is set to 'Enabled: *' (Automated)

Descripción: permite especificar qué hosts de mensajería nativos no se deben cargar. Deshabilitado (0): Google Chrome cargará todos los hosts de mensajería nativos instalados. El estado recomendado para esta configuración es: Habilitado con un valor de *

NOTA: Esto debe manejarse con cuidado. Si una extensión está habilitada, pero no puede comunicarse con su código de back-end, podría comportarse de manera extraña, lo que da como resultado tickets de soporte técnico + carga de soporte.

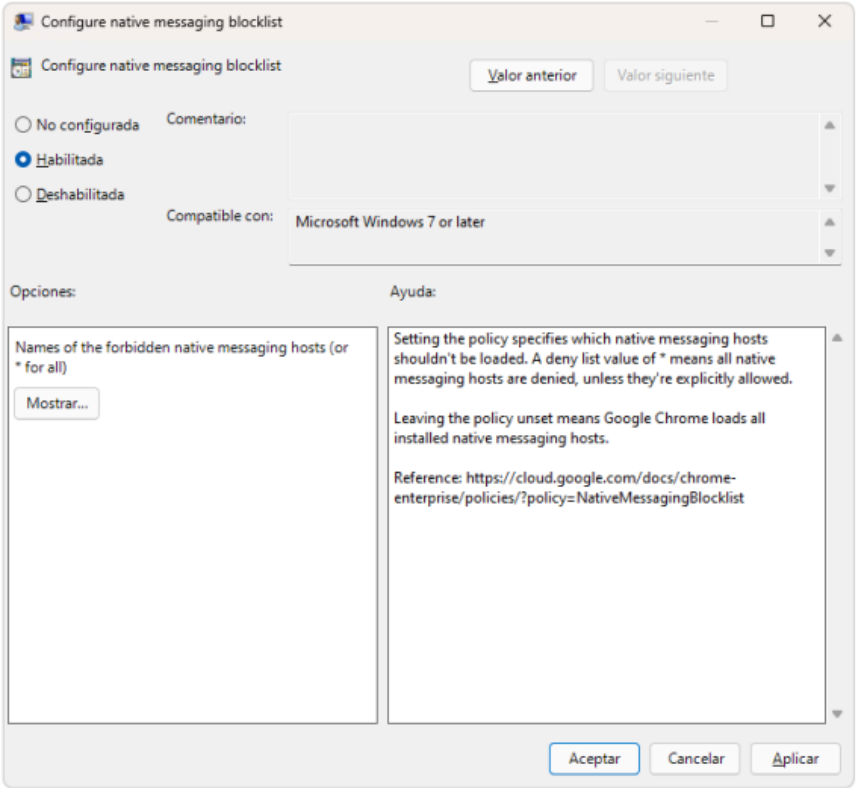
Justificación: Para mantener la coherencia con las directivas de complementos y extensiones, la mensajería nativa debe incluirse en la lista de bloqueo de forma predeterminada, lo que requiere la aprobación administrativa explícita de las aplicaciones para la inclusión en la lista de permitidos. Un ejemplo de una aplicación que utiliza mensajería nativa es el administrador de contraseñas 1Password. Impacto: Un valor de lista de bloqueo de "*" significa que todos los hosts de mensajería nativos están en la lista de bloqueados, a menos que se enumeren explícitamente en la lista de permitidos.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en *:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\NativeMessagingBlocklist:1
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Habilitado y el valor de * establecido en Nombres de los hosts de mensajería nativos prohibidos.

```
Computer Configuration\Polices\Administrative Templates\Google Chrome\Native
Messaging\Configure native messaging blocklist
```



2.6 Password manager

2.6.1 (L1) Ensure 'Enable saving passwords to the password manager' is Explicitly Configured (Manual)

Descripción: Google Chrome tiene un administrador de contraseñas integrado para almacenar las contraseñas de los usuarios. Chrome utilizará la autenticación local para permitir que los usuarios obtengan acceso a estas contraseñas. El estado recomendado para esta configuración es: Establecido explícitamente en Habilitado (1) o Deshabilitado (0) en función de las necesidades de la organización.

NOTA: Si eliges Habilitar esta configuración, revisa Inhabilitar la sincronización de datos con Google y asegúrate de que esta configuración esté configurada para cumplir con los requisitos de la organización.

Justificación: El administrador de contraseñas de Google Chrome está habilitado de forma predeterminada y cada organización debe revisar y determinar si desea permitir que los usuarios almacenen contraseñas en el navegador. Si se utiliza otra solución en lugar de la opción integrada de Chrome, la organización debe configurar la opción en Deshabilitado.

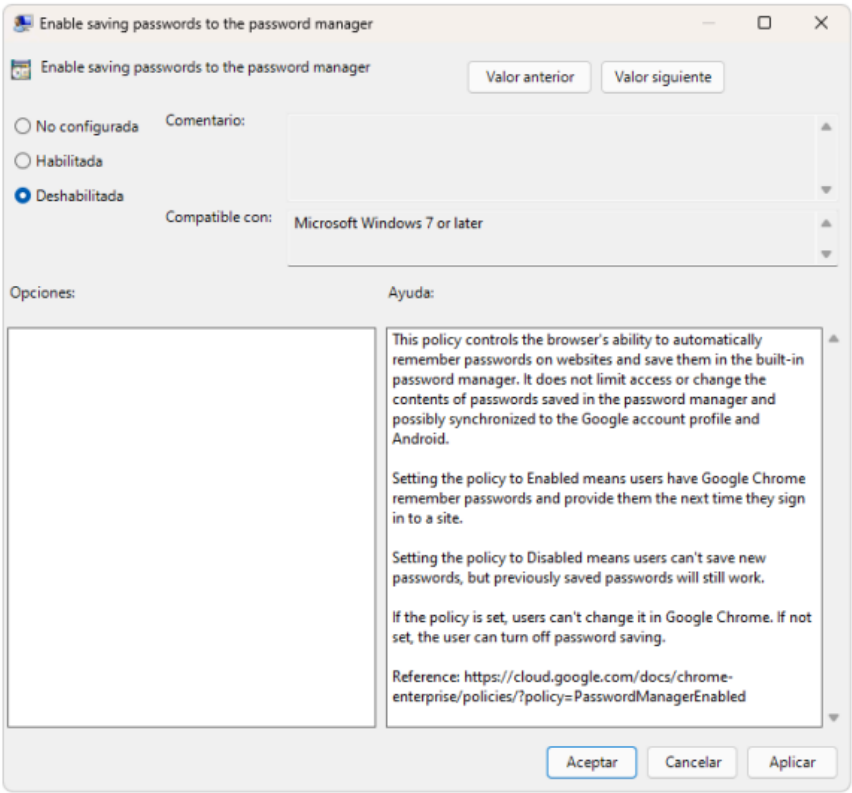
Impacto: Dependiente de la organización.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 0 o 1 (dependiente de la organización):

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:PasswordManagerEnabled
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, configure la siguiente opción para cumplir los requisitos de la organización:

```
Computer Configuration\Polices\Administrative Templates\Google\Google
Chrome\Password manager\Enable saving passwords to the password manager
```



2.7 Printing

2.7.1 (L1) Ensure 'Enable Google Cloud Print Proxy' is set to 'Disabled' (Automated)

Descripción: esta configuración permite que Google Chrome actúe como proxy entre Google Cloud Print y las impresoras heredadas conectadas al equipo. El estado recomendado para esta configuración es: Deshabilitado (0)

Justificación: Al deshabilitar esta opción, se evitará que los usuarios impriman documentos desde dispositivos no administrados en la impresora de una organización.

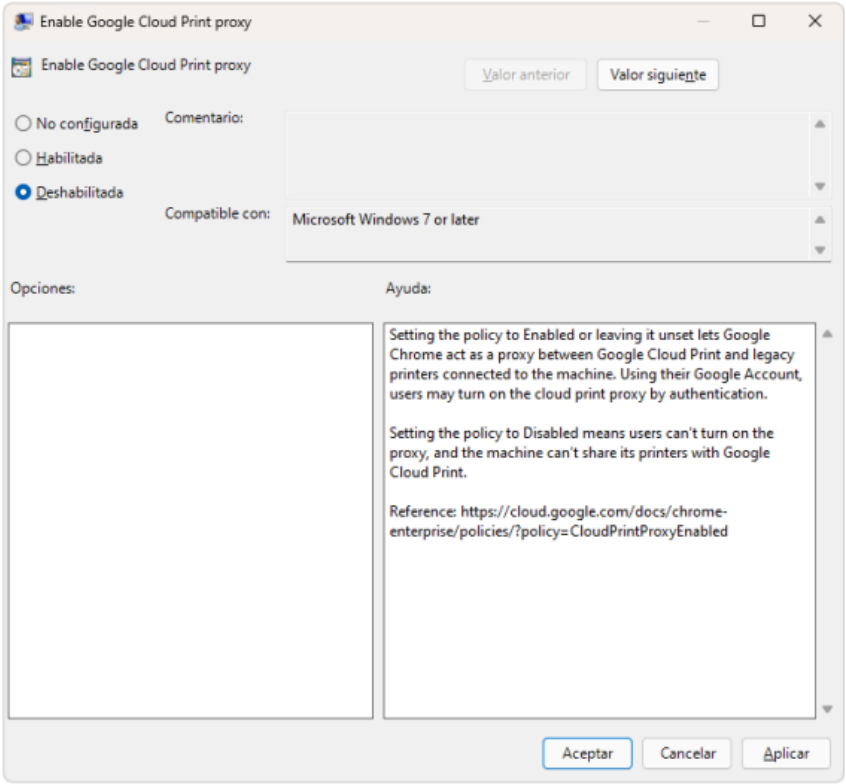
Impacto: Si esta configuración está inhabilitada, los usuarios no podrán habilitar el proxy y el equipo no podrá compartir sus impresoras locales con Google Cloud Print.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:CloudPrintProxyEnabled
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Deshabilitada:

```
Computer Configuration\Polices\Administrative Templates\Google\Google
Chrome\Printing\Enable Google Cloud Print Proxy
```



2.8 Remote access (Chrome Remote Desktop)

En esta sección, se ofrecen recomendaciones específicas para configurar el Escritorio remoto de Chrome.

2.8.1 Ensure 'Allow remote access connections to this machine' is set to 'Disabled' (Manual)

Descripción: se trata de una configuración para el escritorio remoto de Chrome. Si esta configuración está deshabilitada, el servicio de host de acceso remoto no se puede iniciar ni configurar para aceptar conexiones entrantes.

- Deshabilitado (0): Impedir las conexiones de acceso remoto a esta máquina
- Habilitado (1): Permitir conexiones de acceso remoto a esta máquina

El estado recomendado para esta configuración es: Deshabilitado (0)

Justificación: Solo se deben utilizar sistemas de acceso remoto aprobados.

NOTA: Si se aprueba el uso de Escritorio remoto de Chrome y es obligatorio, se puede ignorar esta configuración.

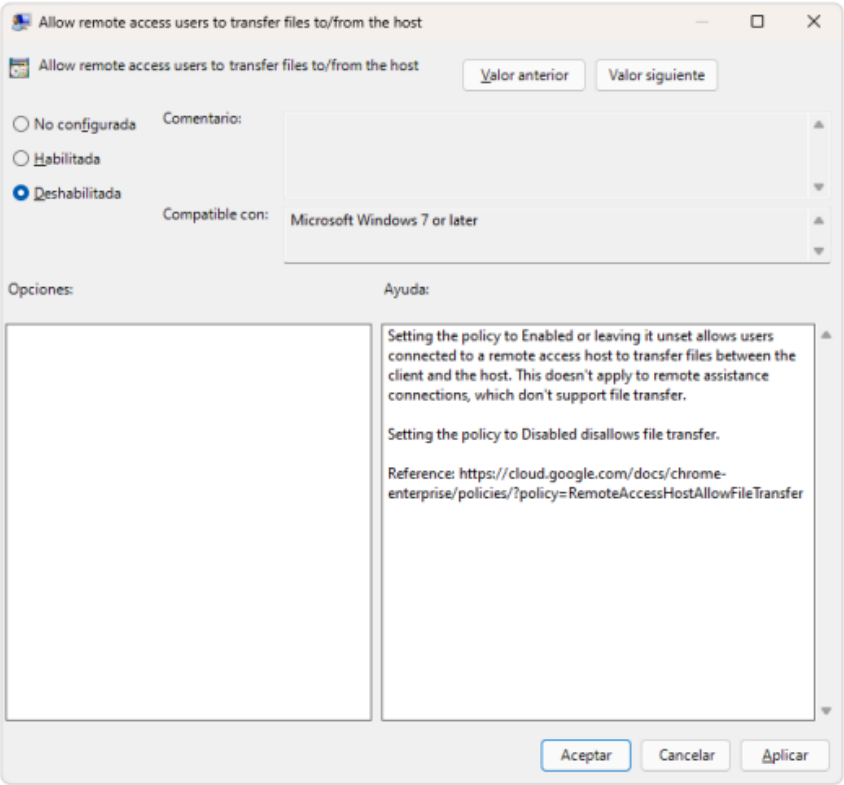
Impacto: Esta configuración inhabilitará el Escritorio remoto de Chrome. En general, la mayoría de las empresas no utilizan el Escritorio remoto de Chrome, por lo que deshabilitarlo no debería tener ningún impacto.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:RemoteAccessHostAllowRemot
eAccessConnections
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Deshabilitada:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\Remote Access\Allow remote access connections to this machine
```



2.8.2 (L1) Ensure 'Allow remote users to interact with elevated windows in remote assistance sessions' is set to 'Disabled' (Automated)

Descripción: Google Chrome se puede configurar para ejecutar el host de asistencia remota en un proceso con permisos de uiAccess. Esto permite a los usuarios remotos interactuar con ventanas elevadas en el escritorio del usuario local. Si esta configuración está deshabilitada, el host de asistencia remota se ejecutará en el contexto del usuario. Además, los usuarios remotos no pueden interactuar con ventanas elevadas en el escritorio. El estado recomendado para esta configuración es: Deshabilitado (0)

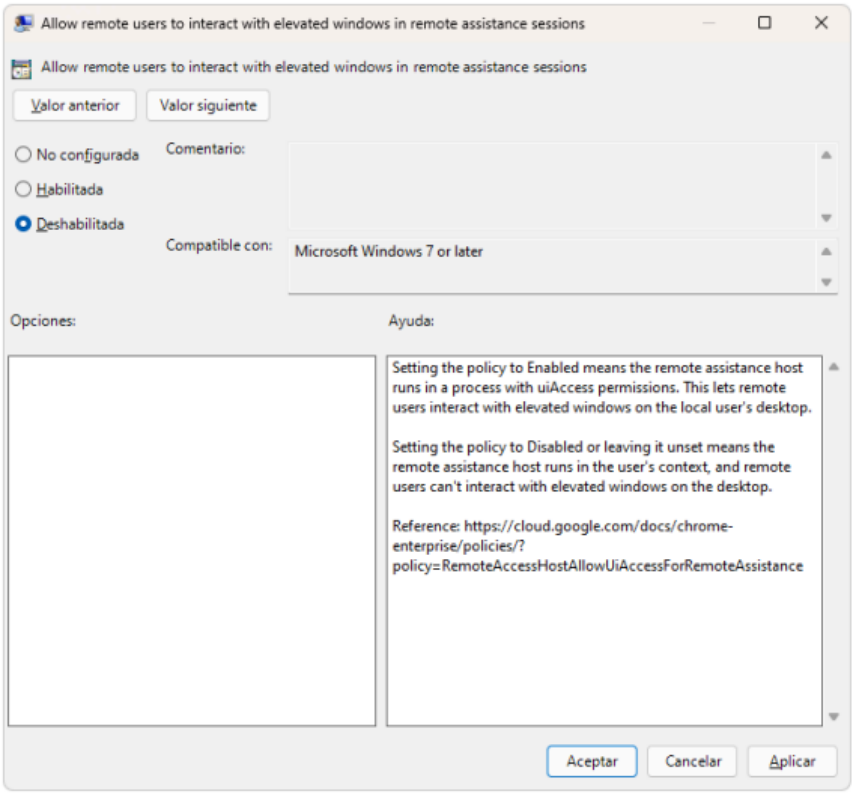
Justificación: Los usuarios remotos no podrán escalar privilegios. Impacto: Ninguno: este es el comportamiento predeterminado.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 0:

```
HKEY LOCAL MACHINE\SOFTWARE\Policies\Google\Chrome:RemoteAccessHostAllowUiAcc
essForRemoteAssistance
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Deshabilitada:

```
Computer Configuration\Polices\Administrative Templates\Google\Google
Chrome\Remote access\Allow remote users to interact with elevated windows in
remote assistance sessions
```



2.8.3 (L1) Ensure 'Configure the required domain names for remote access clients' is set to 'Enabled' with a domain defined (Manual)

Descripción: Chrome permite configurar una lista de dominios que pueden acceder al sistema del usuario. Cuando está habilitado, los sistemas remotos solo pueden conectarse si son uno de los dominios especificados enumerados. Establecer esto en una lista vacía (Deshabilitado) permite que los sistemas remotos de cualquier dominio se conecten al sistema de este usuario. El estado recomendado para esta configuración es: Habilitado (1) y al menos un conjunto de dominios

NOTA: La lista de dominios es específica de la organización. Justificación: Se restringirán las conexiones de asistencia a distancia.

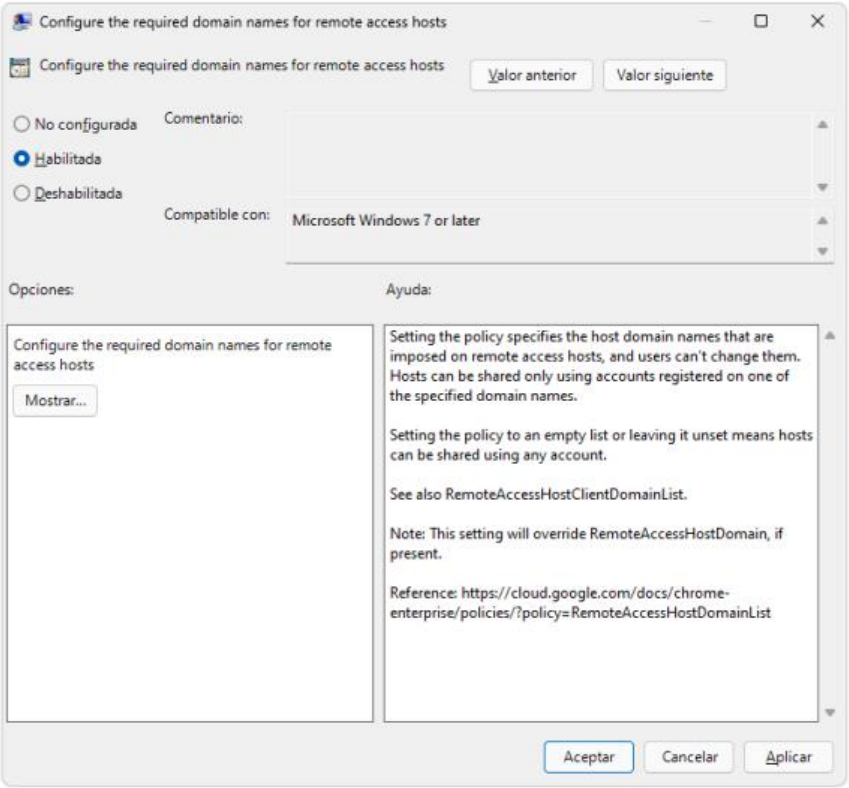
Impacto: Si esta configuración está habilitada, solo los sistemas de los dominios especificados pueden conectarse al sistema del usuario.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta ruta de acceso del Registro no existirá si se establece en Deshabilitado:

```
HKEY LOCAL MACHINE\SOFTWARE\Policies\Google\Chrome\RemoteAccessHostClientDoma
inList
```

Corrección: Para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Habilitado e introduzca un dominio específico de la organización (por ejemplo, nodomain.local):

```
Computer Configuration\Polices\Administrative Templates\Google\Google
Chrome\Remote access\Configure the required domain names for remote access
clients
```



2.8.4 (L1) Ensure 'Enable curtaining of remote access hosts' is set to 'Disabled' (Automated)

Descripción: esta configuración permite que alguien físicamente presente en el equipo host vea lo que está haciendo un usuario mientras se está realizando una conexión remota. Si esta configuración está deshabilitada, los dispositivos físicos de entrada y salida de un host se habilitan mientras hay una conexión remota en curso. El estado recomendado para esta configuración es: Deshabilitado (0)

Justificación: Si hay una sesión remota en curso, el usuario físicamente presente en la máquina host podrá ver lo que está haciendo un usuario remoto.

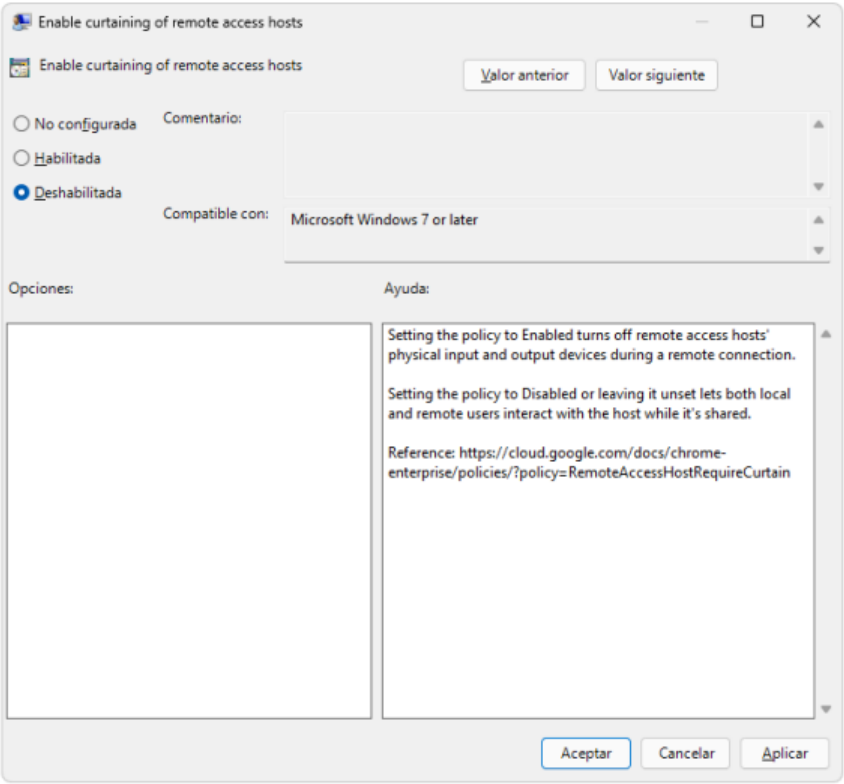
Impacto: Ninguno: este es el comportamiento predeterminado.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:RemoteAccessHostRequireCur
tain
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Deshabilitada:

```
Computer Configuration\Polices\Administrative Templates\Google\Google
Chrome\Remote access\Enable curtaining of remote access hosts
```



2.8.5 (L1) Ensure 'Enable firewall traversal from remote access host' is set to 'Disabled' (Automated)

Descripción: Chrome permite el uso de servidores STUN, lo que permite a los clientes remotos descubrir y conectarse a una máquina incluso si están separados por un firewall. Al deshabilitar esta función, junto con el filtrado de conexiones UDP salientes, la máquina solo permitirá conexiones desde máquinas dentro de la red local. El estado recomendado para esta configuración es: Deshabilitado (0)

Justificación: Si esta configuración está habilitada, los clientes remotos pueden detectar y conectarse a estas máquinas incluso si están separadas por un firewall.

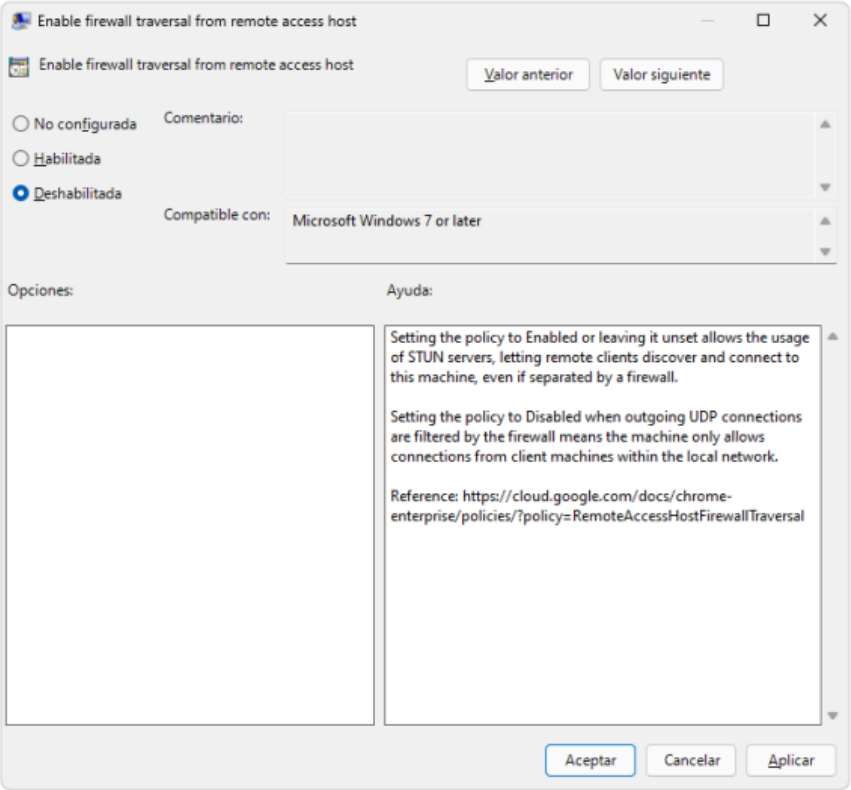
Impacto: Si esta configuración está deshabilitada y el firewall filtra las conexiones UDP salientes, esta máquina solo permitirá conexiones desde máquinas cliente dentro de la red local.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:RemoteAccessHostFirewallTr
aversal
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Deshabilitada:

```
Computer Configuration\Polices\Administrative Templates\Google\Google
Chrome\Remote access\Enable firewall traversal from remote access host
```



2.8.6 (L1) Ensure 'Enable or disable PIN-less authentication for remote access hosts' is set to 'Disabled' (Automated)

Descripción: Chrome permite a un usuario inhabilitar el uso de la autenticación con PIN especificado por el usuario y, en su lugar, emparejar clientes y hosts durante el tiempo de conexión. El estado recomendado para esta configuración es: Deshabilitado (0)

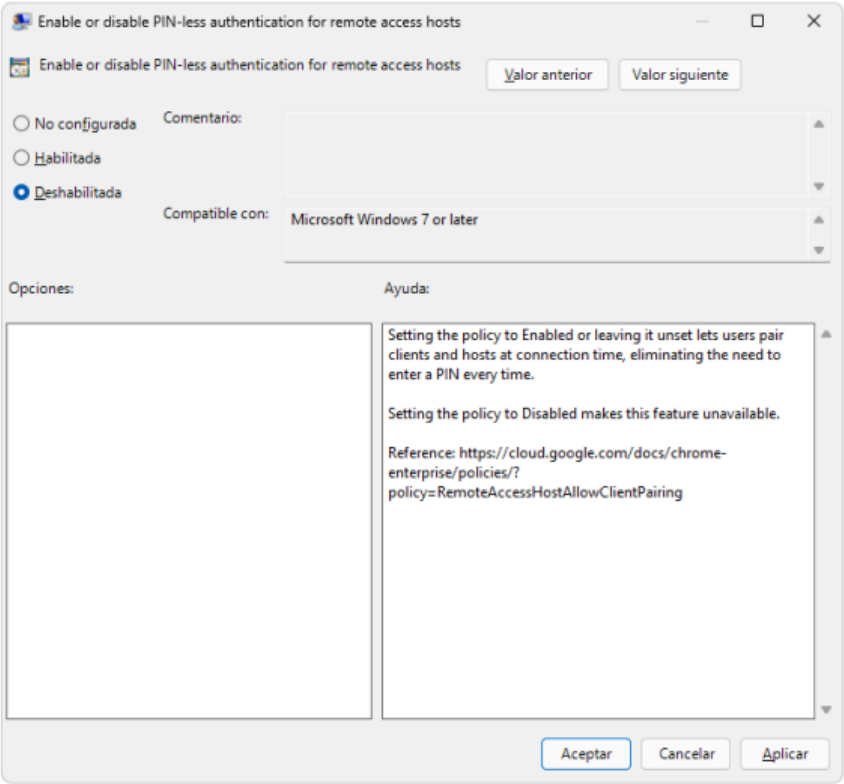
Justificación: Si esta configuración está habilitada, los usuarios pueden optar por emparejar clientes y hosts en el momento de la conexión, lo que elimina la necesidad de ingresar un PIN cada vez.

Impacto: Si esta configuración está deshabilitada, los usuarios deberán ingresar el PIN cada vez. Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:RemoteAccessHostAllowClien
tPairing
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Deshabilitada:

```
Computer Configuration\Polices\Administrative Templates\Google\Google
Chrome\Remote access\Enable or disable PIN-less authentication for remote
access hosts
```



2.8.7 (L1) Ensure 'Enable the use of relay servers by the remote access host' is set to 'Disabled'. (Automated)

Descripción: Google Chrome permite el uso de servidores de retransmisión cuando los clientes intentan conectarse a este equipo y no hay una conexión directa disponible.

- Deshabilitar (0): No se permite el uso de servidores de retransmisión por parte del host de acceso remoto
- Habilitado (1): Se permite el uso de servidores de retransmisión por parte del host de acceso remoto El estado recomendado para esta configuración es: Deshabilitado (0)

Justificación: Los servidores de retransmisión no se utilizarán para eludir las restricciones del firewall.

Impacto: Si esta configuración está deshabilitada, los clientes remotos no pueden utilizar servidores de retransmisión para conectarse a esta máquina.

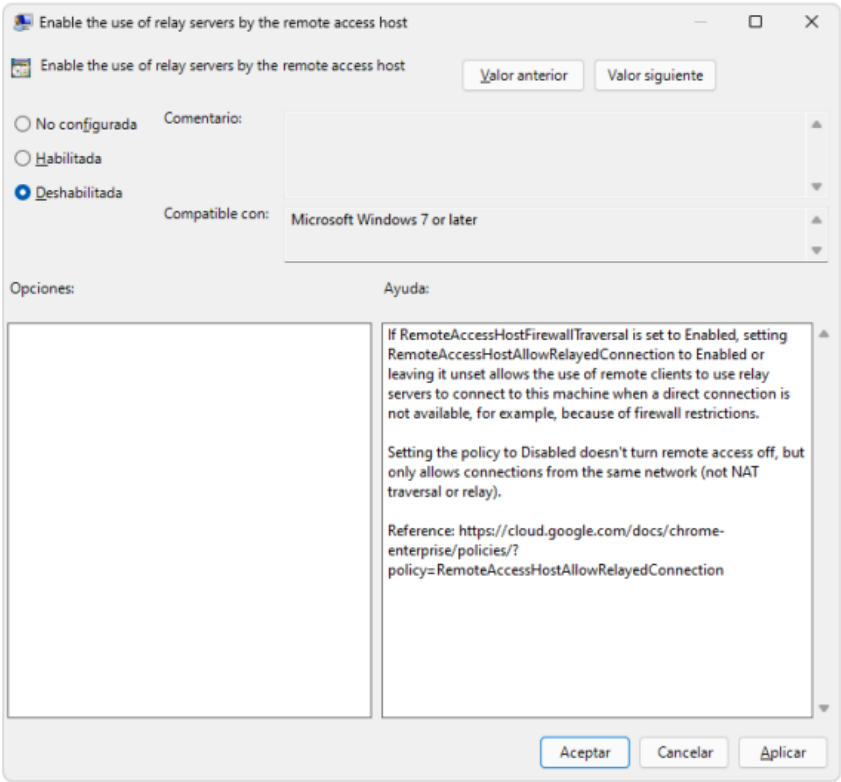
NOTA: Si se establece esta opción en Desactivado, no se desactiva el acceso remoto, sino que solo se permiten conexiones desde la misma red (no NAT transversal ni relé).

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:RemoteAccessHostAllowRelay
edConnection
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Deshabilitada:

```
Computer Configuration\Polices\Administrative Templates\Google\Google
Chrome\Remote access\Enable the use of relay servers by the remote access
host
```



2.9 First-Party Sets Settings

Controla las directivas de la característica Conjuntos de origen

2.9.1 (L1) Ensure 'Enable First-Party Sets' Is Disabled (Manual)

Descripción: esta directiva controla el acceso a los conjuntos de origen. Los conjuntos de origen son una forma de que los sitios declaren relaciones entre sí y permitan el acceso limitado a las cookies entre sitios para fines específicos de cara al usuario. Se puede configurar para:

- Deshabilitado (0): Deshabilitar conjuntos de origen para todos los usuarios afectados
- Habilitado (1): Habilitar conjuntos de origen para todos los usuarios afectados

Justificación: La configuración de esta directiva no permitirá que los sitios declaren las relaciones que les permiten acceder a las cookies entre sitios.

Impacto: esto puede provocar un comportamiento inesperado a medida que un usuario se mueve entre sitios afiliados.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de

directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:FirstPartySetsEnabled
```

Corrección: para establecer la configuración recomendada a través de GP, establezca la siguiente ruta de acceso de la interfaz de usuario en Deshabilitado:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\Content settings\Enable Firty-Party Sets
```

2.10 Microsoft Active Directory Management Settings

2.10.1 (L1) Ensure 'Allow automatic sign-in to Microsoft cloud identity providers' Is Enabled (Manual)

Descripción: esta configuración de directiva permite que las cuentas respaldadas por un proveedor de identidades en la nube de Microsoft® (es decir, Microsoft Azure Active Directory o el proveedor de identidades de la cuenta de Microsoft del consumidor) puedan iniciar sesión en las propiedades web con esa identidad automáticamente. Se puede configurar para:

• Deshabilitado (0): Deshabilitar la autenticación en la nube de Microsoft®

• Habilitado (1): Habilitar la autenticación en la nube de Microsoft® Si el valor de CloudAPAuthEnabled no se cambia con respecto al valor predeterminado, se comportará como si estuviera deshabilitado.

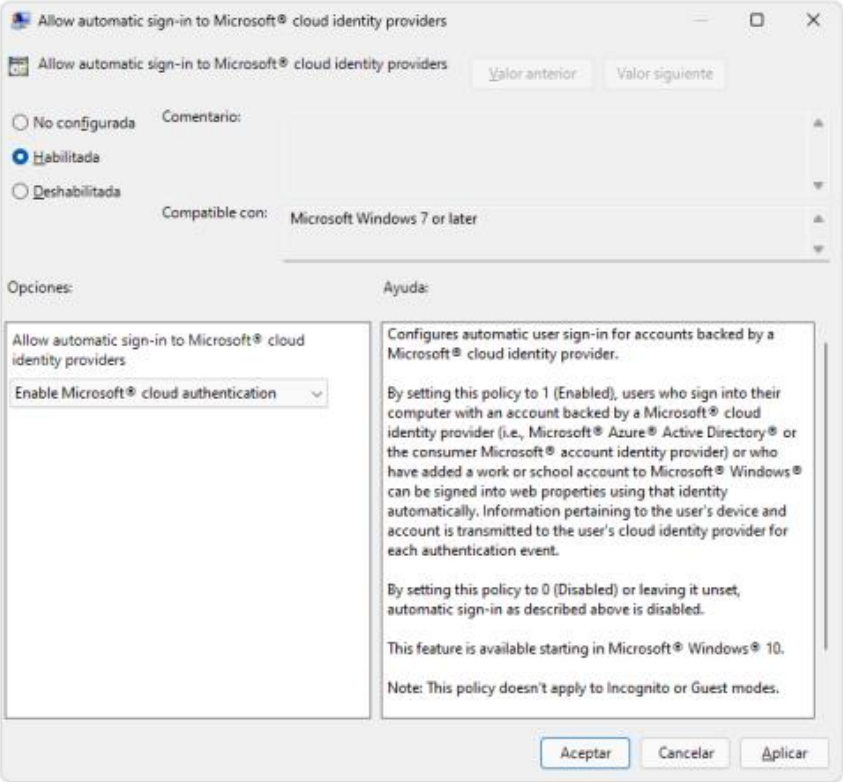
Justificación: la habilitación de esta configuración de directiva permite a los usuarios usar Microsoft Cloud Authentication para cualquier sitio que requiera CA (Cloud Authentication) y no requiera una extensión. Impacto: No debe haber ningún impacto para el usuario.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 1:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:CloudAPAuthEnabled
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Habilitada: Habilite la autenticación en la nube de Microsoft®:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\Microsoft® Active Directory® management settings\Allow automatic sign-
in to Microsoft® cloud identity providers
```



2.11 (L1) Ensure 'Allow download restrictions' is set to 'Enabled: Block malicious downloads' (Automated)

Descripción: Google Chrome puede bloquear ciertos tipos de descargas y no permitirá que los usuarios omitan las advertencias de seguridad, según la clasificación de Navegación segura.

- Sin restricciones especiales. Predeterminado. (0, Deshabilitado) (Predeterminado)
- Bloquee las descargas maliciosas y los tipos de archivos peligrosos. (1)
- Bloquee descargas maliciosas, descargas poco comunes o no deseadas y tipos de archivos peligrosos. (2)
- Bloquear todas las descargas. (3)
- Bloquear descargas maliciosas. Recomendado. (4) El estado recomendado para esta configuración es: Habilitado con un valor de Bloquear descargas maliciosas. Recomendado. (4)

NOTA: Estas restricciones se aplican a las descargas activadas desde el contenido de la página web, así como al enlace de descarga... opción de menú. No se aplican a la

descarga de la página que se muestra actualmente ni a guardar como PDF desde las opciones de impresión.

Justificación: Se evitará que los usuarios descarguen tipos de archivos maliciosos y no podrán eludir las advertencias de seguridad. Impacto: si esta configuración está habilitada, se permiten todas las descargas, excepto las que llevan advertencias de navegación segura. Se trata de descargas que han sido identificadas como peligrosas o de una fuente peligrosa por el motor de inteligencia global de Navegación segura de Google.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 4

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:DownloadRestrictions
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Habilitada: Bloquear descargas malintencionadas. Recomendado.:

```
Computer Configuration\Polices\Administrative Templates\Google\Google
Chrome\Allow download restrictions
```

2.12 (L2) Ensure 'Allow proceeding from the SSL warning page' is set to 'Disabled' (Automated)

Descripción: esta configuración controla si un usuario puede ir a una página web cuando se ha producido una advertencia de certificado SSL no válido. El estado recomendado para esta configuración es: Deshabilitado (0)

Justificación: Los sitios protegidos por SSL siempre deben reconocerse como válidos en el explorador web. Permitir que un usuario tome la decisión de si parece haber un certificado no válido podría exponer a una organización a los usuarios que visitan un sitio que, de otro modo, no es seguro o es de naturaleza malintencionada.

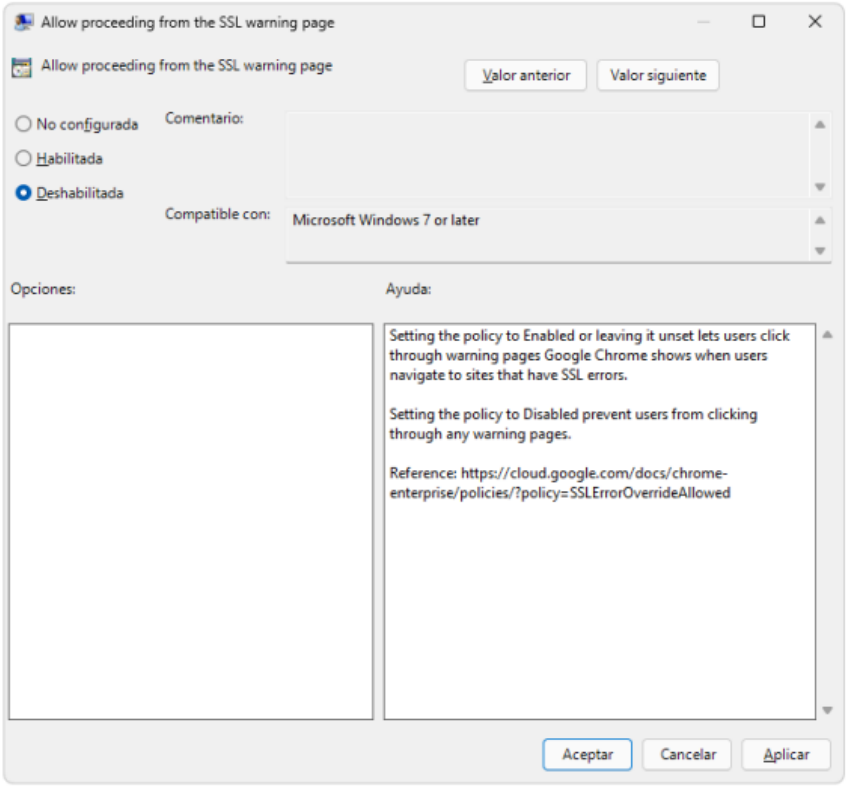
Impacto: Los usuarios no podrán hacer clic más allá del error de certificado no válido para ver el sitio web.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:SSLErrorOverrideAllowed
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Deshabilitada:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\Allow proceeding from the SSL warning page
```



2.13 (L1) Ensure 'Disable proceeding from the Safe Browsing warning page' is set to 'Enabled' (Automated)

Descripción: Google proporciona el servicio de navegación segura. Muestra una página de advertencia cuando los usuarios navegan a sitios marcados como potencialmente malintencionados. Deshabilitado (0): los usuarios pueden optar por continuar con el sitio marcado después de que aparezca la advertencia. El estado recomendado para esta configuración es: Habilitado (1)

Justificación: Las páginas web maliciosas están ampliamente difundidas en Internet y representan la amenaza más importante para el usuario en la actualidad. Se impedirá a los usuarios navegar a contenidos web potencialmente maliciosos.

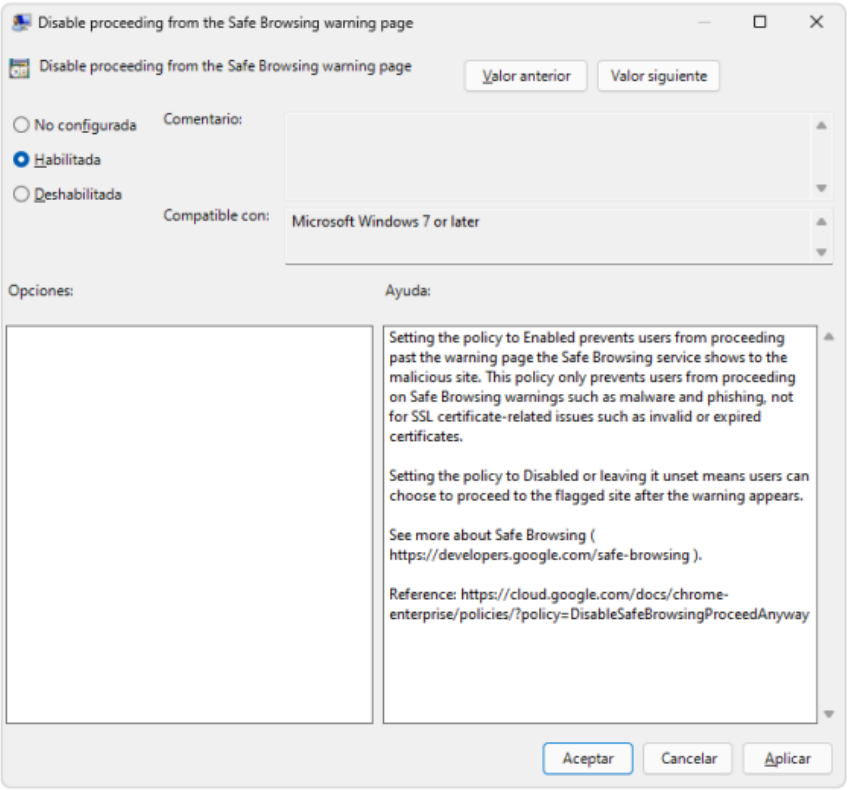
Impacto: Al habilitar esta configuración, los usuarios no pueden pasar de todos modos de la página de advertencia al sitio malintencionado. En algunos casos, los sitios legítimos podrían bloquearse y se impediría el acceso de los usuarios.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 1:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:DisableSafeBrowsingProceed
Anyway
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Habilitada:

```
Computer Configuration\Polices\Administrative Templates\Google\Google
Chrome\Safe Browsing settings\Disable proceeding from the Safe Browsing
warning page
```



2.14 (L1) Ensure 'Require Site Isolation for every site' is set to 'Enabled' (Automated)

Descripción: esta configuración controla si cada sitio web se cargará en su propio proceso. Deshabilitado (0): no desactiva el aislamiento del sitio, pero permite a los usuarios optar por no participar. El estado recomendado para esta configuración es: Habilitado (1)

Justificación: Chrome cargará cada sitio web en su propio proceso. Incluso si un sitio omite la política de sameorigin, la seguridad adicional ayudará a evitar que el sitio robe sus datos de otro sitio web.

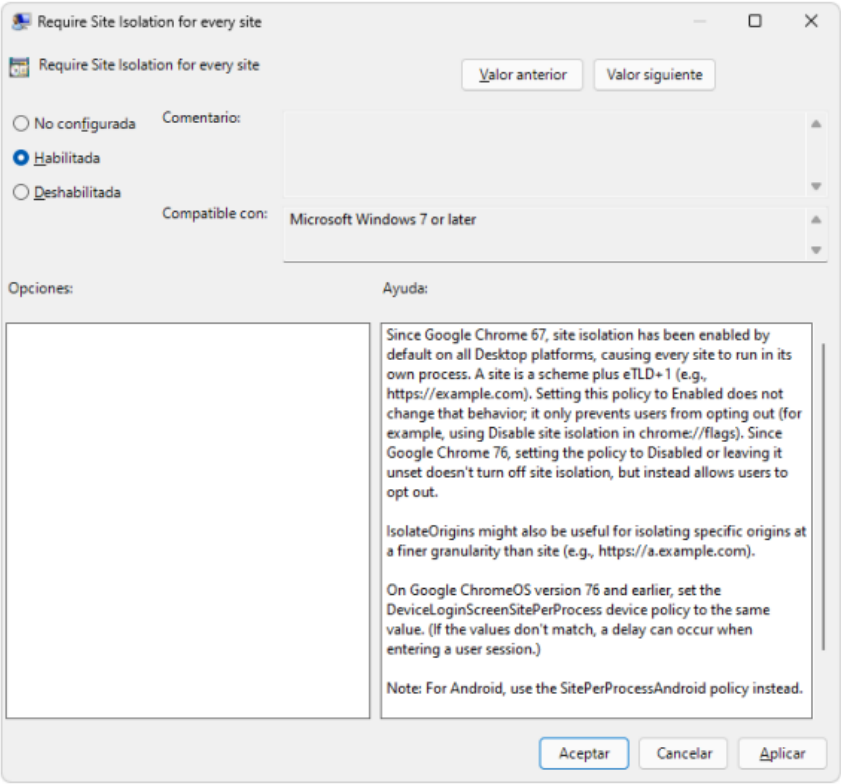
Impacto: si la directiva está habilitada, cada sitio se ejecutará en su propio proceso, lo que hará que el sistema use más memoria. Es posible que desee consultar la configuración de directiva Habilitar el aislamiento de sitios para orígenes especificados para obtener lo mejor de ambos mundos (aislamiento e impacto limitado para los usuarios) mediante el uso de Habilitar aislamiento de sitios para orígenes especificados con una lista de los sitios que desea aislar.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 1:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:SitePerProcess
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Habilitada:

```
Computer Configuration\Polices\Administrative Templates\Google\Google
Chrome\Require Site Isolation for every site
```



2.15 (L2) Ensure 'Force Google SafeSearch' is set to 'Enabled' (Automated)

Descripción: esta configuración garantiza que los resultados de búsqueda web con Google se realicen con SafeSearch configurado como siempre activo. Inhabilitado significa que SafeSearch en la Búsqueda de Google no está aplicado. El estado recomendado para esta configuración es: Habilitado (1)

Justificación: Se debe prohibir permitir que los resultados de búsqueda presenten sitios que puedan tener contenido malintencionado para ayudar a garantizar que los usuarios no visiten accidentalmente sitios que son más propensos a contenido malintencionado, incluidos spyware, adware y virus.

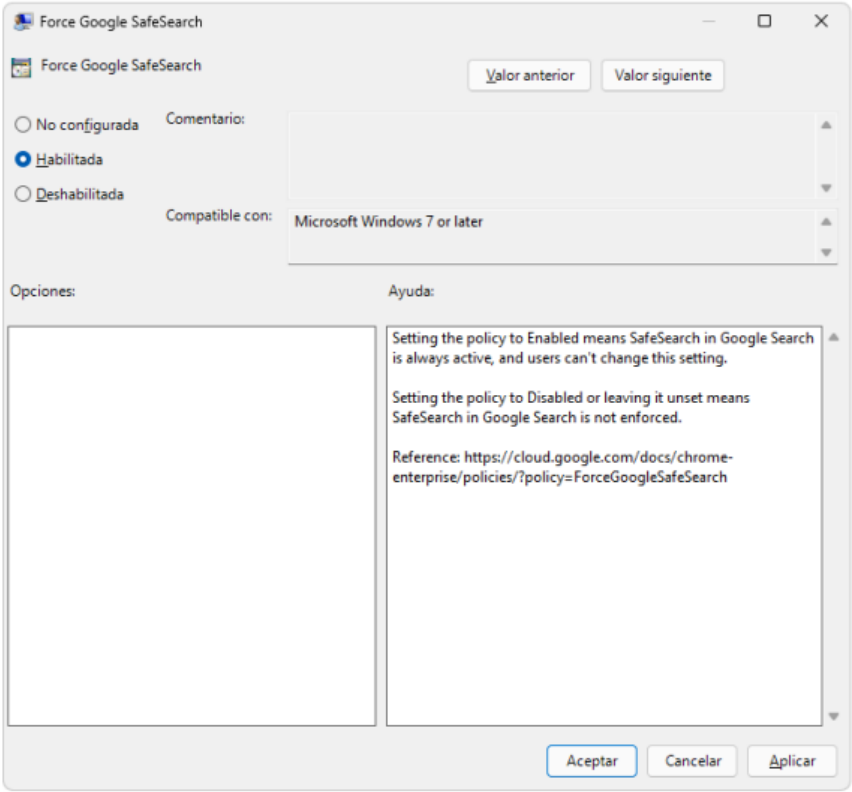
Impacto: los resultados de búsqueda de los usuarios se filtrarán y no se mostrará contenido como texto, vídeos e imágenes para adultos.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 1:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:ForceGoogleSafeSearch
```

Corrección: para establecer la configuración recomendada a través de GP, establezca la siguiente ruta de acceso de la interfaz de usuario en Habilitada:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\Force Google SafeSearch
```



2.16 (L1) Ensure 'Notify a user that a browser relaunch or device restart is recommended or required' is set to 'Enabled: Show a recurring prompt to the user indication that a relaunch is required' (Automated)

Descripción: Google Chrome puede notificar a los usuarios que debe reiniciarse para aplicar una actualización pendiente una vez que haya transcurrido el período de notificación definido por la recomendación Establecer el período de tiempo para las notificaciones de actualización.

- Mostrar un mensaje recurrente al usuario que indica que se recomienda un reinicio (1)
- Mostrar un mensaje recurrente al usuario que indica que se requiere un reinicio (2)

Deshabilitado: Google Chrome indica al usuario que se necesita un reinicio a través de cambios sutiles en su menú. El estado recomendado para esta configuración es: Habilitado con un valor de Mostrar un mensaje recurrente al usuario que indica que es necesario reiniciar (2)

Justificación: el usuario final recibirá una notificación en la que se le informará de que se ha aplicado una actualización y de que el explorador debe reiniciarse para que se complete la actualización. Una vez que las actualizaciones han sido enviadas por la

organización, es pertinente que la actualización se aplique lo antes posible. Al habilitar esta notificación, se asegurará de que los usuarios reinicien su navegador de manera oportuna.

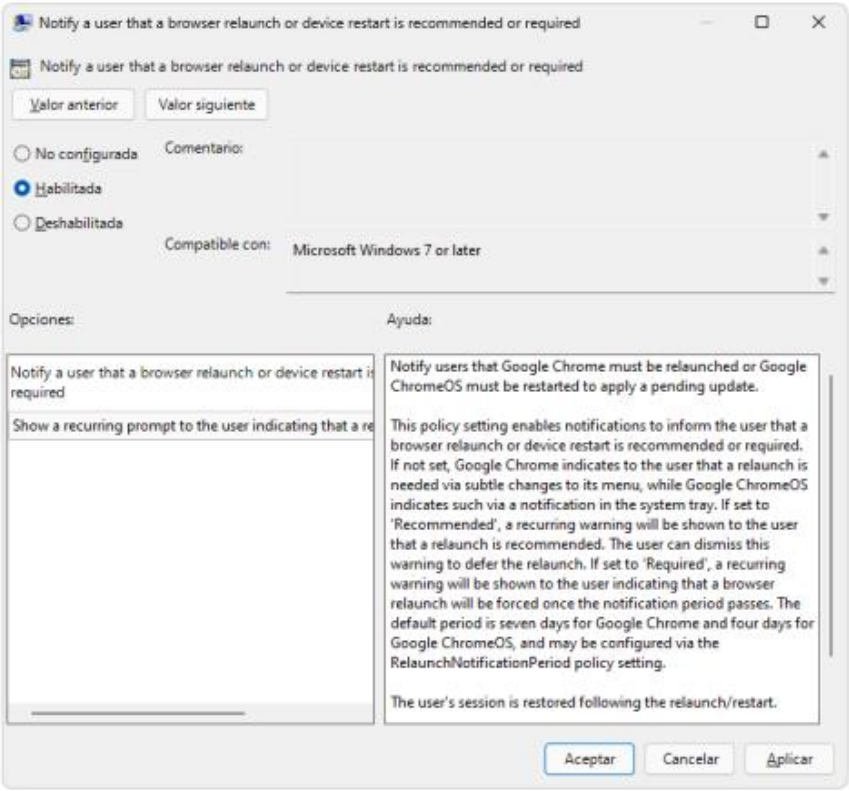
Impacto: se mostrará una advertencia recurrente al usuario que indica que se forzará el reinicio del navegador una vez que pase el período de notificación. La sesión del usuario se restaura después del reinicio de Google Chrome.

Auditoría: Navegue hasta la ruta de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 2:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:RelaunchNotification
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Habilitada: Mostrar un mensaje recurrente al usuario que indique que se requiere un reinicio:

```
Computer Configuration\Polices\Administrative Templates\Google\Google
Chrome\Notify a user that a browser relaunch or device restart is recommended
or required
```



2.17 (L1) Ensure 'Proxy settings' is set to 'Enabled' and does not contain "ProxyMode": "auto_detect" (Automated)

Descripción: Google Chrome ofrece la funcionalidad de configurar los ajustes del proxy mediante la detección automática mediante WPAD (Web Proxy Auto-Discovery Protocol). Al establecer esta opción, se configuran los ajustes de proxy para Chrome y las aplicaciones de ARC, que ignoran todas las opciones relacionadas con el proxy especificadas desde la línea de comandos.

Deshabilitado (0): Permite a los usuarios elegir la configuración de su proxy. El estado recomendado para esta configuración es: Habilitado y el valor de ProxyMode no está establecido en auto_detect

Justificación: los atacantes pueden abusar de la funcionalidad de configuración automática de WPAD para proporcionar a los equipos un archivo PAC que especifique un proxy web no autorizado bajo su control.

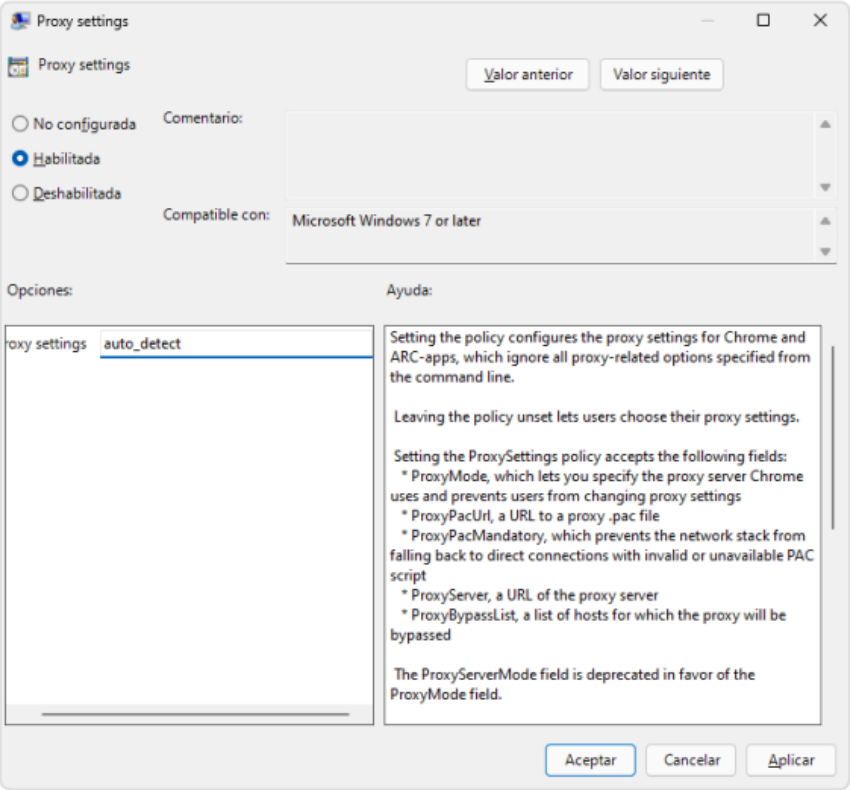
Impacto: Si la directiva está habilitada, la configuración del proxy ya no se detectará mediante WPAD.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro que NO debe establecerse en auto_detect:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:ProxyMode
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, asegúrese de que la siguiente ruta de acceso de la interfaz de usuario esté establecida en "Habilitada" y que el valor de ProxyMode no esté establecido en auto_detect:

```
Computer Configuration\Polices\Administrative Templates\Google\Google
Chrome\Proxy settings
```


Proxy settings
Proxy settings
Valor anterior
Valor siguiente
No configurada
Habilitada
Deshabilitada
Comentario:
Compatible con:
Microsoft Windows 7 or later
Opciones:
Ayuda:
roxy settings
auto_detect
Setting the policy configures the proxy settings for Chrome and ARC-apps, which ignore all proxy-related options specified from the command line.
Leaving the policy unset lets users choose their proxy settings.
Setting the ProxySettings policy accepts the following fields:
* ProxyMode, which lets you specify the proxy server Chrome uses and prevents users from changing proxy settings
* ProxyPacUrl, a URL to a proxy .pac file
* ProxyPacMandatory, which prevents the network stack from falling back to direct connections with invalid or unavailable PAC script
* ProxyServer, a URL of the proxy server
* ProxyBypassList, a list of hosts for which the proxy will be bypassed
The ProxyServerMode field is deprecated in favor of the ProxyMode field.
Aceptar
Cancelar
Aplicar

2.18 (L2) Ensure 'Require online OCSP/CRL checks for local trust anchors' is set to 'Enabled' (Automated)

Descripción: Google Chrome realiza comprobaciones de revocación de certificados de servidor que validan correctamente y están firmados por certificados de CA instalados localmente. Si Google Chrome no puede obtener información sobre el estado de la revocación, dichos certificados se considerarán revocados ("error grave"). Inhabilitado: Google Chrome utiliza la configuración existente de verificación de revocación en línea. El estado recomendado para esta configuración es: Habilitado (1)

Justificación: Los certificados siempre se validarán.

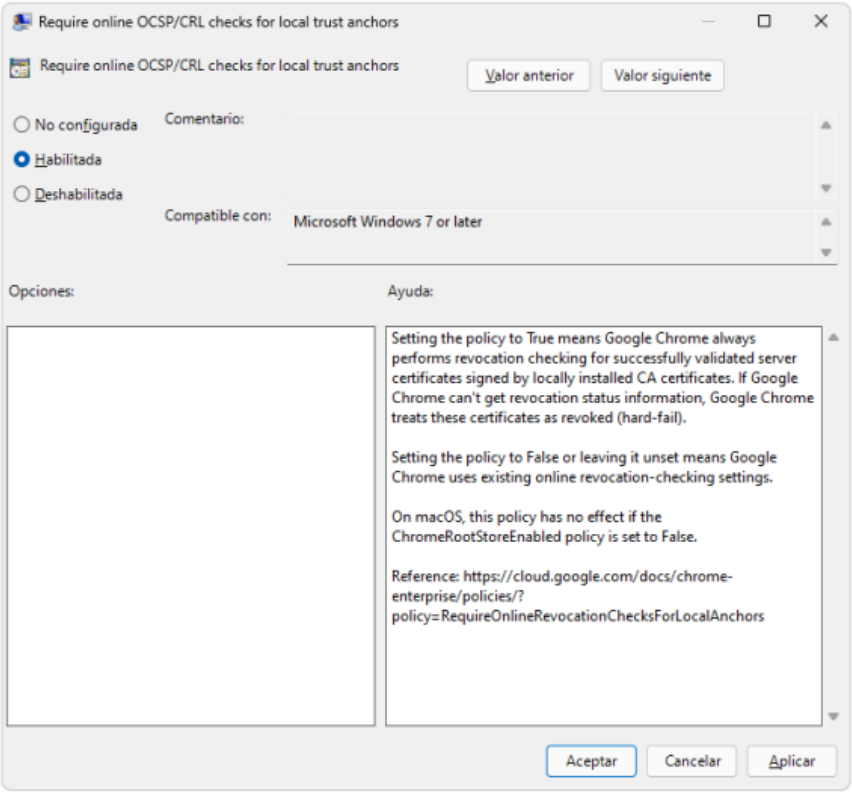
Impacto: Se realizará una comprobación de revocación de los certificados de servidor que se validen correctamente y estén firmados por certificados de CA instalados localmente. si el servidor OCSP deja de funcionar, esto fallará de forma difícil e impedirá navegar a esos sitios.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 1:

```
HKEY LOCAL MACHINE\SOFTWARE\Policies\Google\Chrome:RequireOnlineRevocationChe
cksForLocalAnchors
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Habilitada:

```
Computer Configuration\Polices\Administrative Templates\Google\Google
Chrome\Require online OCSP/CRL checks for local trust anchors
```



2.19 (L1) Ensure 'Set the time period for update notifications' is set to 'Enabled: 86400000' (Automated)

Descripción: Google Chrome permite establecer el período de tiempo, en milisegundos, durante el cual se notifica a los usuarios que debe reiniciarse para aplicar una actualización pendiente. Si no se establece, o se deshabilita, se utiliza el período predeterminado de 604800000 milisegundos (7 días). El estado recomendado para esta configuración es: Habilitado con el valor 86400000 (1 día)

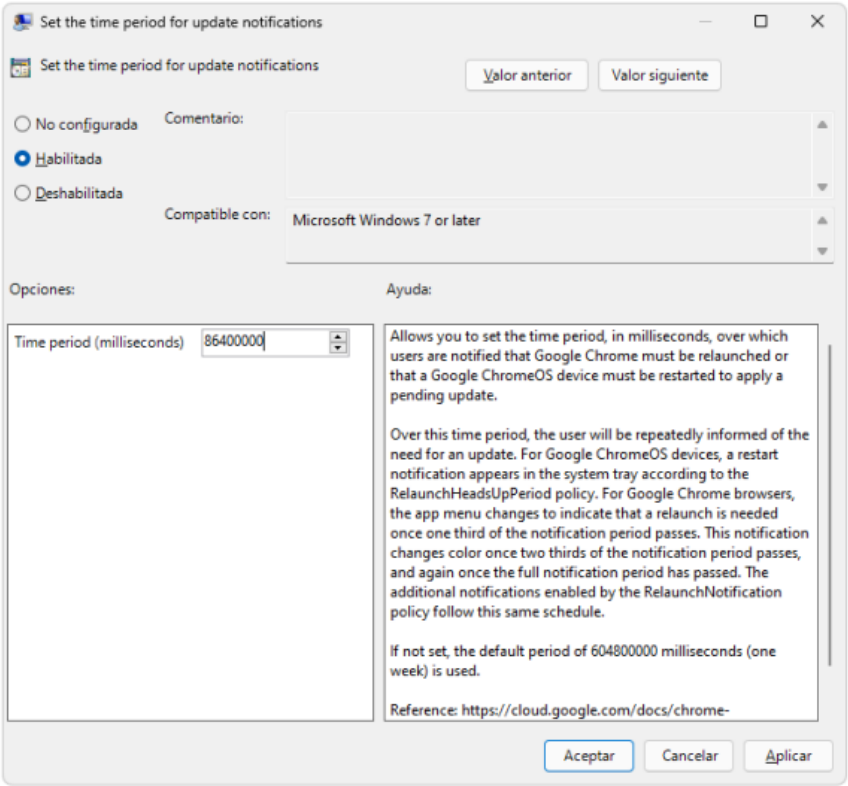
Justificación: esta configuración es una notificación para el usuario final que le informa de que se ha aplicado una actualización y que el explorador debe reiniciarse para que se complete la actualización. Una vez que las actualizaciones han sido impulsadas por la organización, es pertinente que dicha actualización entre en vigor lo antes posible. Al habilitar esta notificación, los usuarios se asegurarán de reiniciar el navegador de manera oportuna.

Impacto: Después de este período de tiempo, se informará repetidamente al usuario de la necesidad de una actualización hasta que se complete el reinicio del navegador.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:RelaunchNotificationPeriod
```

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 86400000.

```
Computer Configuration\Polices\Administrative Templates\Google\Google
Chrome\Set the time period for update notifications
```



2.20 (L1) Ensure 'Allow Web Authentication requests on sites with broken TLS certificates' Is Disabled (Automated)

Descripción: esta configuración de directiva controla la API de WebAuthn y su interacción con los sitios que tienen un certificado TLS roto. Se puede configurar para:

• Deshabilitado (0): no permite solicitudes de API de WebAuthn en sitios con certificados TLS rotos.

• Habilitado (1): permite solicitudes de API de WebAuthn en sitios con certificados TLS rotos. Si el valor de AllowWebAuthnWithBrokenTlsCerts no se cambia con respecto al valor predeterminado, se comportará como si estuviera deshabilitado.xempt.

Justificación: La configuración de esta directiva bloqueará la capacidad de autenticarse en cualquier sitio web que no tenga un certificado TLS válido, ya que no se puede verificar la identidad del sitio.

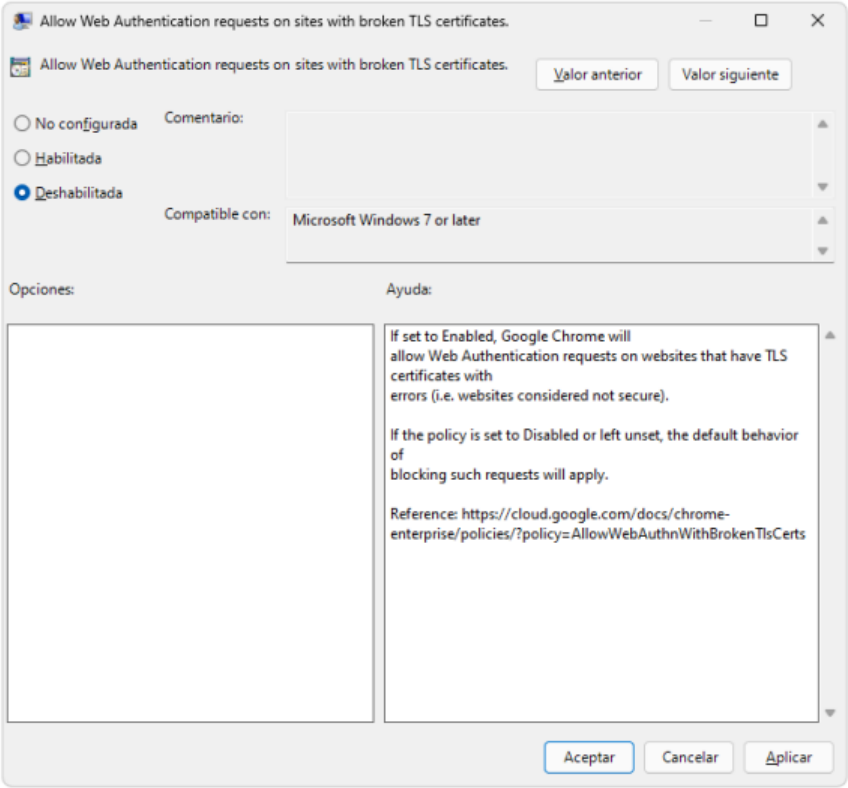
Impacto: No debe haber ningún impacto en el usuario.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:AllowWebAuthnWithBrokenTls
Certs
```

Corrección: para establecer la configuración recomendada a través de GP, establezca la siguiente ruta de acceso de la interfaz de usuario en Deshabilitado:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\Allow Web Authentication requests on sites with broken TLS
certificates.
```



2.21 (L1) Ensure 'Allow reporting of domain reliability related data' Is Disabled (Automated)

Descripción: esta configuración controla los valores predeterminados para el acceso a los permisos del portapapeles desde los sitios. Se puede configurar para:

- Inhabilitado (0): nunca enviar datos de confiabilidad del dominio a Google
- Habilitado (1): los datos de confiabilidad del dominio se pueden enviar a Google según la política de métricas de usuario de Chrome (UMA) Si el valor de DomainReliabilityAllowed no se cambia con respecto al valor predeterminado, se comportará como está habilitado.

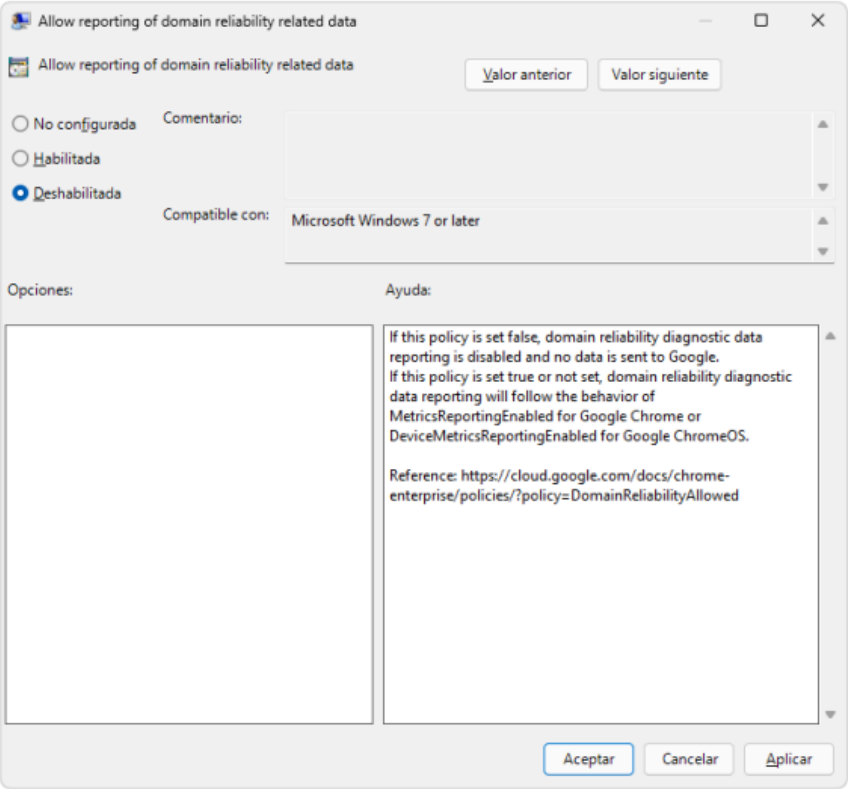
Justificación: Establecer esta directiva en deshabilitada puede detener cualquier fuga accidental de datos. Impacto: No debe haber ningún impacto en el usuario.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:DomainReliabilityAllowed
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Deshabilitada:

```
Computer Configuration\Policies\Administrative Templates\Google Chrome\Allow
reporting of domain reliability related data
```



2.22 (L1) Ensure 'Enable TLS Encrypted ClientHello' Is Enabled (Automated)

Descripción: esta configuración controla los valores predeterminados para usar Encrypted ClientHello (ECH). ECH es una extensión de TLS y encripta el protocolo de enlace inicial con un sitio web que solo puede ser descifrado por ese sitio web. Google Chrome puede, o no, usar ECH en función de 3 factores: compatibilidad con servidores, disponibilidad de registros DNS HTTPS o estado de lanzamiento. Se puede configurar para:

- Deshabilitado (0): deshabilita el experimento ClientHello cifrado TLS
- Habilitado (1): habilita el experimento ClientHello cifrado TLS

Si el valor de EncryptedClientHelloEnabled no se cambia con respecto al valor predeterminado, se comportará como está habilitado.

Justificación: Anteriormente, todos los apretones de manos eran abiertos y podían exponer información confidencial, como el nombre del sitio web al que se está conectando. La configuración de esta política permitirá a Google Chrome utilizar un saludo o protocolo de enlace cifrado con un sitio web en el que sea compatible, por lo que no expondrá información confidencial.

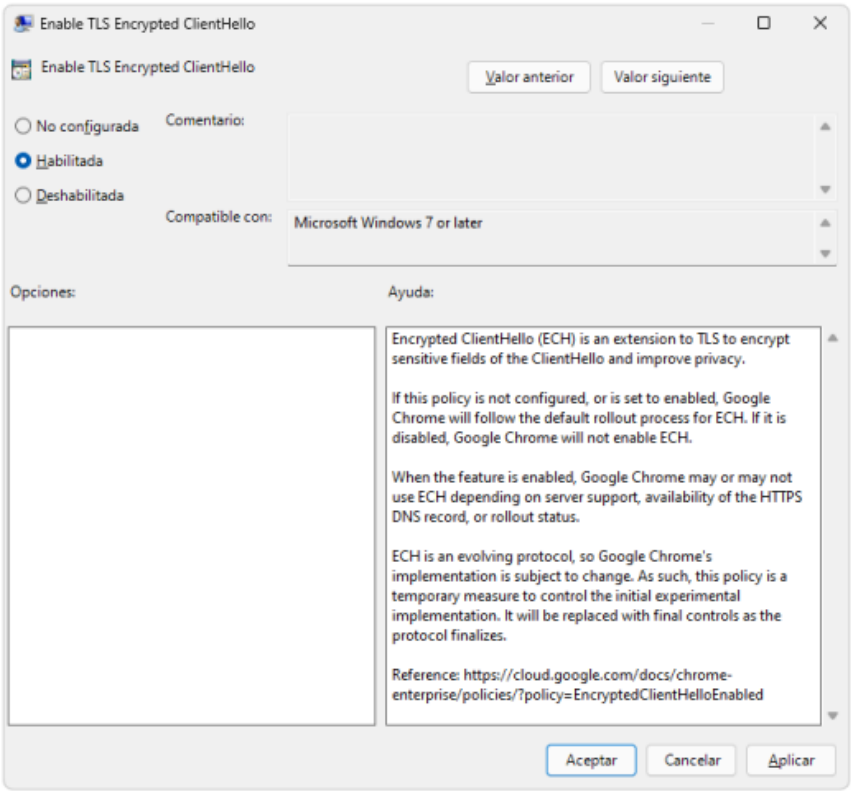
Impacto: No debe haber ningún impacto en el usuario.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 1:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:EncryptedClientHelloEnable
d
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Habilitada:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\Enable TLS Encrypted ClientHello
```



2.23 (L2) Ensure 'Determines whether the built-in certificate verifier will enforce constraints encoded into trust anchors loaded from the platform trust store' Is Enabled (Automated)

Descripción: esta configuración controla las restricciones codificadas en los anclajes de confianza cargados desde el almacén de confianza de la plataforma. Se puede configurar para:

• Deshabilitado (0): no aplicar restricciones en anclajes de confianza agregados localmente

• Habilitado (1): Aplicar restricciones en anclajes de confianza agregados localmente Si el valor de EnforceLocalAnchorConstraintsEnabled no se cambia con respecto al valor predeterminado, se comportará como si estuviera habilitado.

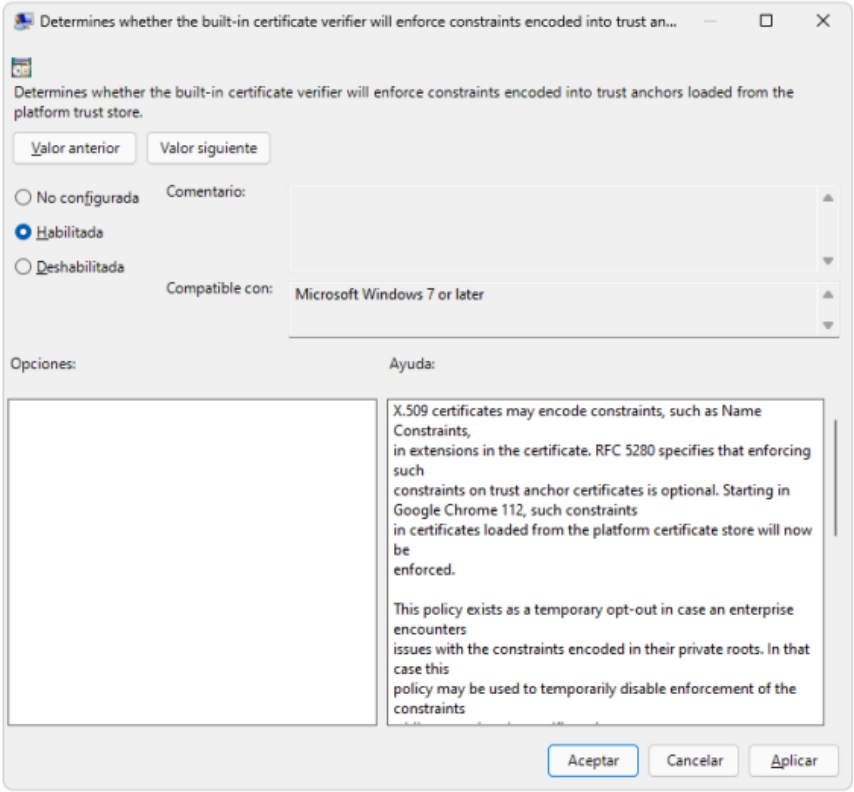
Justificación: La configuración de esta directiva no permitirá el acceso a ningún sitio que no aplique restricciones. Impacto: Habilitar esta opción podría hacer que algunos sitios internos no se carguen correctamente hasta que se actualicen.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 1:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:EnforceLocalAnchorConstrai
ntsEnabled
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Habilitada:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\Determines whether the built-in certificate verifier will enforce
constraints encoded into trust anchors loaded from the platform trust store.
```



2.24 (L1) Ensure 'Keep browsing data when creating enterprise profile by default' Is Enabled (Automated)

Descripción: esta configuración controla la conservación de los datos existentes del navegador cuando se crea un perfil de empresa. Se puede configurar para:

- Deshabilitado (0): no marque la opción para mantener los datos de navegación existentes de forma predeterminada
- Habilitado (1): marque la opción para mantener los datos de navegación existentes de forma predeterminada Si el valor de EnterpriseProfileCreationKeepBrowsingData no se cambia con respecto al valor predeterminado, se comportará como si estuviera habilitado.

Nota: A diferencia de otras configuraciones de directiva, el usuario puede decidir si desea conservar o no los datos de navegación existentes al crear un perfil de empresa.

Justificación: La configuración de esta directiva ofrece al usuario la opción de conservar los datos de navegación anteriores después de configurar un perfil de empresa.

Impacto: Esto no debería tener ningún efecto en el usuario.

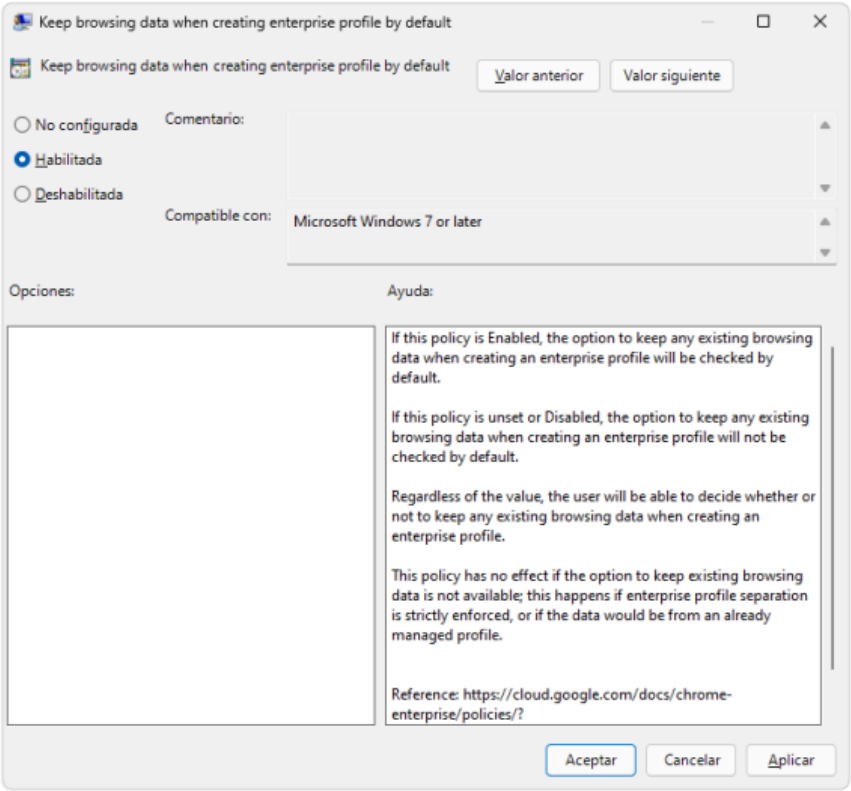
Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de

directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 1:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:EnterpriseProfileCreationK
eepBrowsingData
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Habilitada:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\Keep browsing data when creating enterprise profile by default
```



2.25 (L1) Ensure 'Allow file or directory picker APIs to be called without prior user gesture' Is Disabled (Automated)

Descripción: esta configuración controla la capacidad de llamar a las API web showOpenFilePicker(), showSaveFilePicker() y showDirectoryPicker() sin interacción del usuario. Si el valor de FileOrDirectoryPickerWithoutGestureAllowedForOrigins no se cambia con respecto al valor predeterminado, se comportará como si estuviera deshabilitado.

Justificación: La configuración de esta política permitiría que las URL seleccionadas llamen a las API web showOpenFilePicker(), showSaveFilePicker() y showDirectoryPicker() sin ningún gesto o interacción del usuario. No es necesario establecer esta directiva por este motivo.

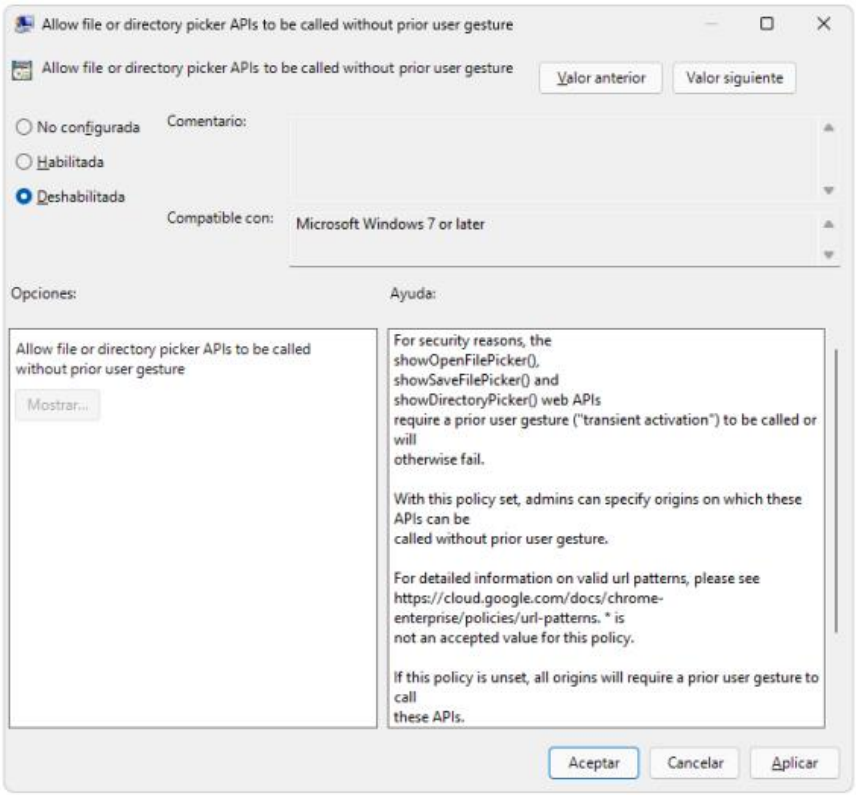
Impacto: la deshabilitación de esta directiva no debería tener ningún impacto en el usuario.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro que no debería existir:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\FileOrDirectoryPickerWitho
utGestureAllowedForOrigins\<number> = <url>
```

Corrección: para establecer la configuración recomendada a través de GP, establezca la siguiente ruta de acceso de la interfaz de usuario en Deshabilitado:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\Allow file or directory picker APIs to be called without prior user
gesture
```



2.26 (L1) Ensure 'Enable Google Search Side Panel' Is Disabled (Automated)

Descripción: esta configuración controla el panel lateral de la Búsqueda de Google. Se puede configurar para:

- Deshabilitado (0): Inhabilitar el panel lateral de la Búsqueda de Google en todas las páginas web
- Habilitado (1): Habilitar el panel lateral de la Búsqueda de Google en todas las páginas web

Justificación: La configuración de esta política no permitirá el panel lateral de la Búsqueda de Google en ninguna página web.

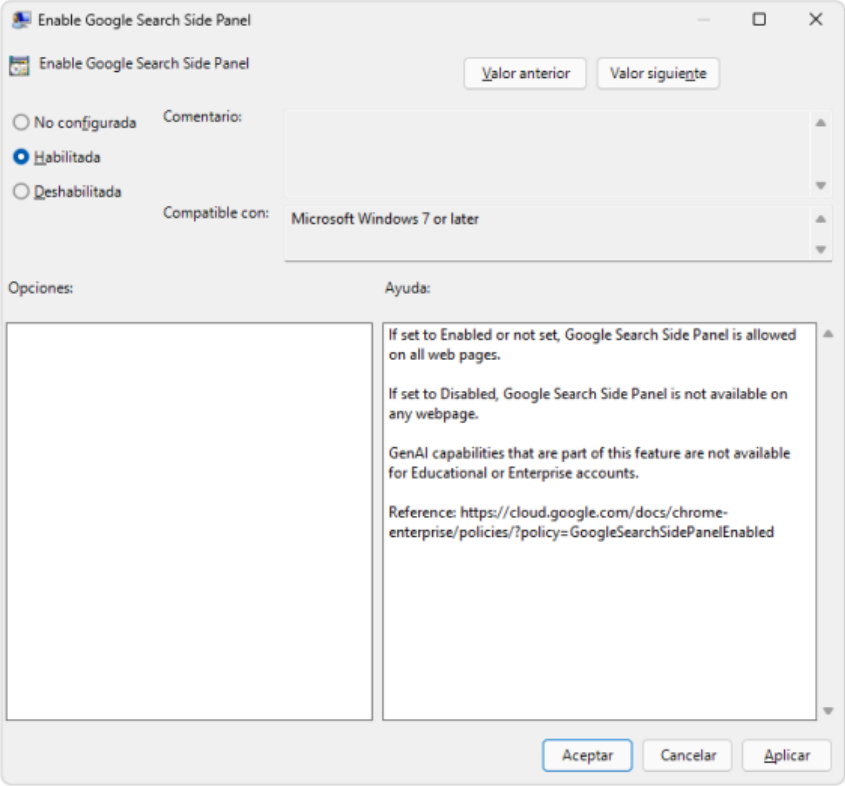
Impacto: Esto no debería tener ningún impacto en el usuario.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:GoogleSearchSidePanelEnabl
ed
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Habilitada:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\Enable Google Search Side Panel
```



2.27 (L1) Ensure 'Http Allowlist' Is Properly Configured (Manual)

Descripción: esta configuración permite a los administradores enumerar sitios específicos que no se actualizarán a HTTPS y no mostrarán un error intersticial si el modo HTTPS-First está habilitado.

Nota: Los comodines (*, [*], etc.) no están permitidos en los listados de URL.

Justificación: La configuración de esta directiva permite a las organizaciones mantener el acceso a servidores que no admiten HTTPS sin tener que deshabilitar el modo HTTPS-First o las actualizaciones de HTTPS.

Impacto: Esto no debe tener un impacto en el usuario.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse individualmente en las direcciones URL permitidas de la organización:

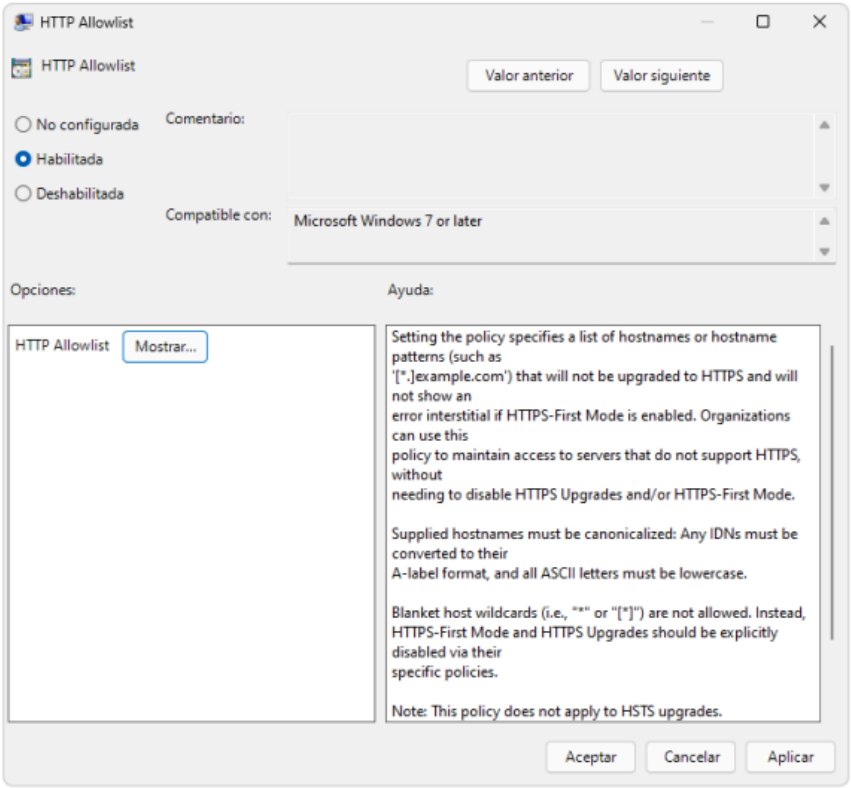
```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\HttpAllowlist\<number> =
<url>
```

Example:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\HttpAllowlist\1 =
www.example.com
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\HttpAllowlist\2 =
[*.]example.edu
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\HttpAllowlist\3 =
www.example.net
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Habilitada y establezca Mostrar en las direcciones URL aprobadas:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\HTTP Allowlist
```



2.28 (L1) Ensure 'Enable automatic HTTPS upgrades' Is Enabled (Automated)

Descripción: esta configuración controla la capacidad de Google Chrome para actualizar a HTTPS desde HTTP mientras navega a determinados sitios. Se puede configurar para:

- Deshabilitado (0): Deshabilitar actualizaciones HTTPS
- Habilitado (1): Se pueden aplicar actualizaciones HTTPS según el estado de inicio de la función

Si el valor de HttpsUpgradesEnabled no se cambia del valor predeterminado, se comportará como si estuviera habilitado. Justificación: Al habilitar esta configuración, se actualizará la conexión a un sitio de HTTP a HTTPS cuando esté disponible, verificando la identidad del sitio visitado.

Impacto: Esto no debería tener ningún impacto en el usuario.

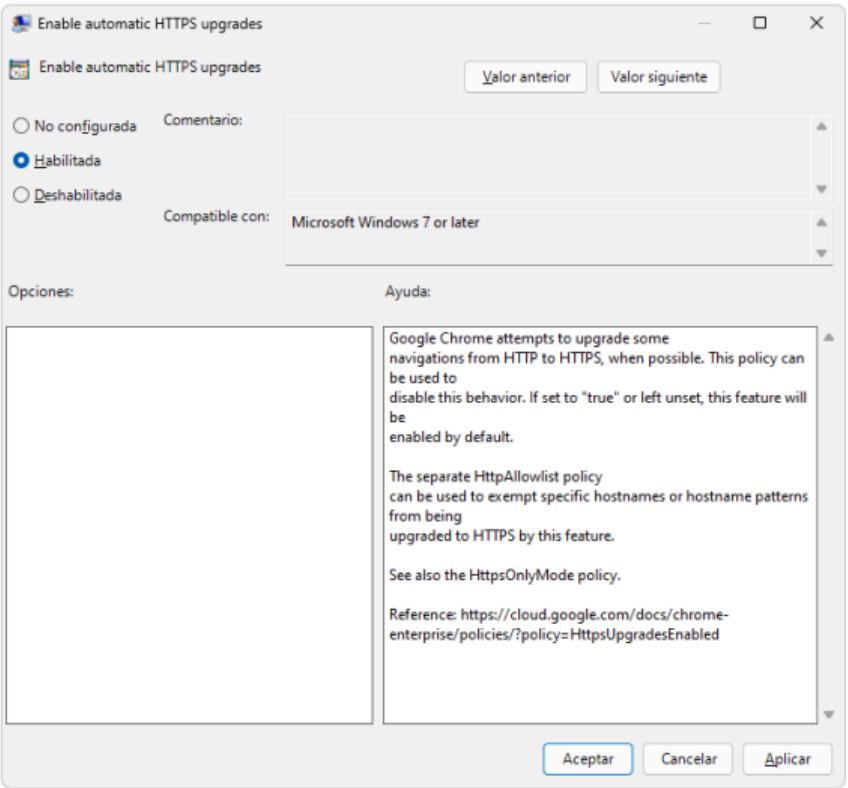
Nota: Si hay sitios o servidores internos que solo usan HTTP, configúrelos en la directiva

Auditoría de HttpAllowlist: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 1:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:HttpsUpgradesEnabled
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Habilitada:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\Enable automatic HTTPS upgrades
```



2.29 (L1) Ensure 'Insecure Hashes in TLS Handshakes Enabled' Is Disabled (Automated)

Descripción: esta configuración controla la capacidad de Google Chrome para permitir hashes heredados o inseguros durante el protocolo de enlace TLS. Se puede configurar para:

- Deshabilitado (0): No permitir hashes inseguros en los protocolos de enlace TLS
- Habilitado (1): Permitir hashes inseguros en los protocolos de enlace TLS Si el valor de InsecureHashesInTLSHandshakesEnabled no se cambia con respecto al valor predeterminado, se comportará como si estuviera habilitado.

Justificación: Si se establece esta política como inhabilitada, se impedirá que Google Chrome utilice hashes inseguros. El uso de hashes inseguros o heredados podría permitir que se expongan datos confidenciales.

Impacto: se bloqueaba la visita de los usuarios a sitios que no admitían hashes más seguros.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:InsecureHashesInTLSHandsha
kesEnabled
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Deshabilitada:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\Insecure Hashes in TLS Handshakes Enabled
```

2.30 (L1) Ensure 'Enable Renderer App Container' Is Enabled (Automated)

Descripción: esta configuración controla la capacidad de Google Chrome para permitir que se use el sandbox de Render App Container mientras se navega por determinados sitios. Se puede configurar para:

- Deshabilitado (0): Deshabilitar el espacio aislado del contenedor de aplicaciones del renderizador
- Habilitado (1): Habilitar el espacio aislado del contenedor de aplicaciones del procesador Si el valor de RendererAppContainerEnabled no se cambia del valor predeterminado, se comportará como si estuviera habilitado.

Justificación: La inhabilitación de esta política debilitaría el espacio aislado que Google Chrome utiliza para el proceso de procesamiento y tendría un efecto perjudicial en la seguridad y la estabilidad del navegador. Esta política debe estar habilitada para mantener la seguridad y la estabilidad.

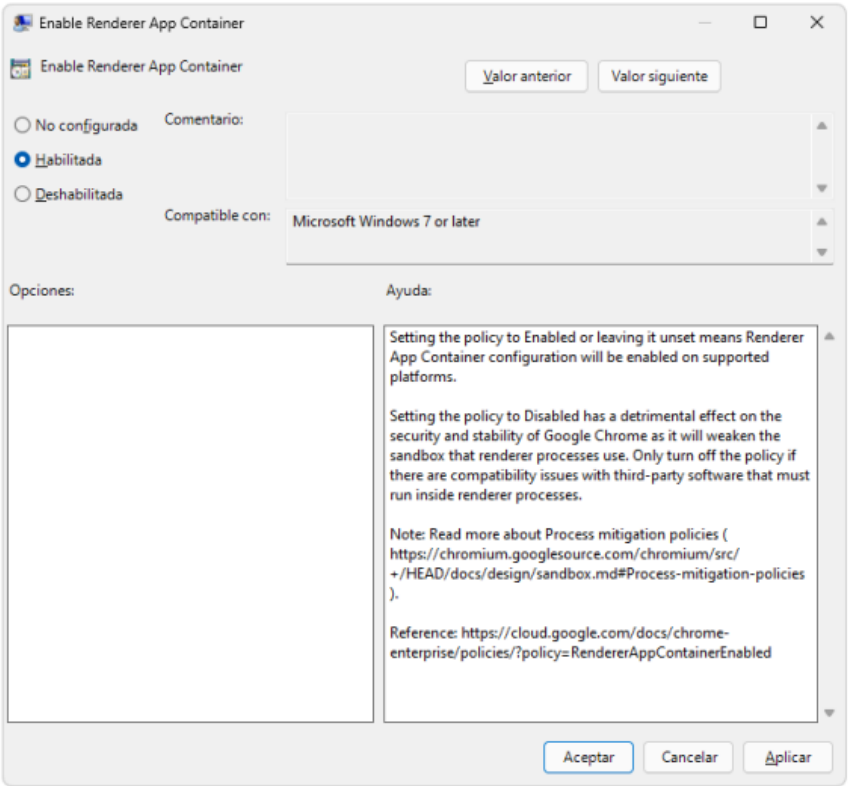
Impacto: Esto solo afectaría a los usuarios si hay software de terceros que debe ejecutarse dentro de los procesos del renderizador.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 1:

```
HKEY LOCAL MACHINE\SOFTWARE\Policies\Google\Chrome:RendererAppContainerEnable
d
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Habilitado:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\Enable Renderer App Container
```



2.31 (L1) Ensure 'Enable strict MIME type checking for worker scripts' Is Enabled (Automated)

Descripción: esta configuración controla la capacidad de Google Chrome para actualizar a HTTPS desde HTTP mientras navega a determinados sitios. Se puede configurar para:

• Deshabilitado (0): los scripts para trabajadores (Web Workers, Service Workers, etc.) utilizan una comprobación de tipo MIME laxa. Los scripts de trabajo con tipos MIME heredados, como text/ascii, funcionarán.

• Habilitado (1): los scripts para trabajadores (Web Workers, Service Workers, etc.) requieren un tipo MIME de JavaScript, como text/javascript. Se rechazarán los scripts de trabajo con tipos MIME heredados, como text/ascii. Si el valor de StrictMimetypeCheckForWorkerScriptsEnabled no se cambia con respecto al valor predeterminado, se comportará como si estuviera habilitado.

Justificación: La configuración de esta directiva requerirá que los scripts de trabajo usen tipos MIME de JavaScript más seguros y estrictos, y se rechazarán los que tengan tipos MIME heredados.

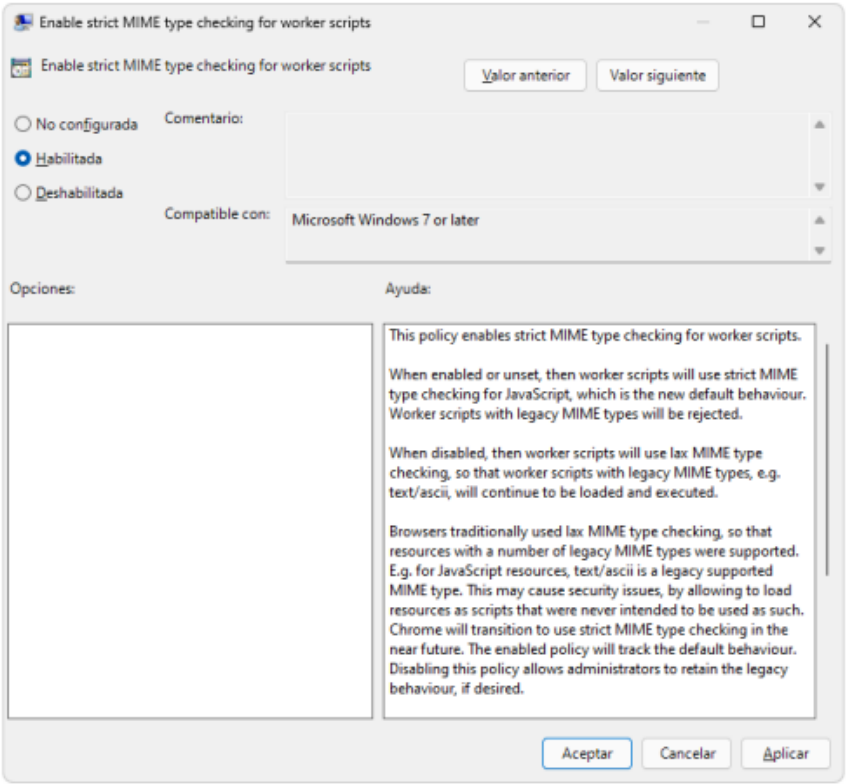
Impacto: Esto no debería tener ningún impacto en los usuarios.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 1:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:StrictMimetypeCheckForWork
erScriptsEnabled
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Habilitada:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\Enable strict MIME type checking for worker scripts
```



2.32 Ensure 'Allow remote debugging' is set to 'Disabled' (Automated)

Descripción: esta configuración de directiva controla si los usuarios pueden usar la depuración remota. Esta característica permite la depuración remota de contenido en vivo en un dispositivo Windows 10 o posterior desde una computadora con Windows o macOS. El estado recomendado para esta configuración es: Deshabilitado.

Justificación: La desactivación de la depuración remota mejora la seguridad y protege las aplicaciones del acceso no autorizado. Algunas herramientas de ataque pueden aprovechar esta función para extraer información o insertar código malicioso.

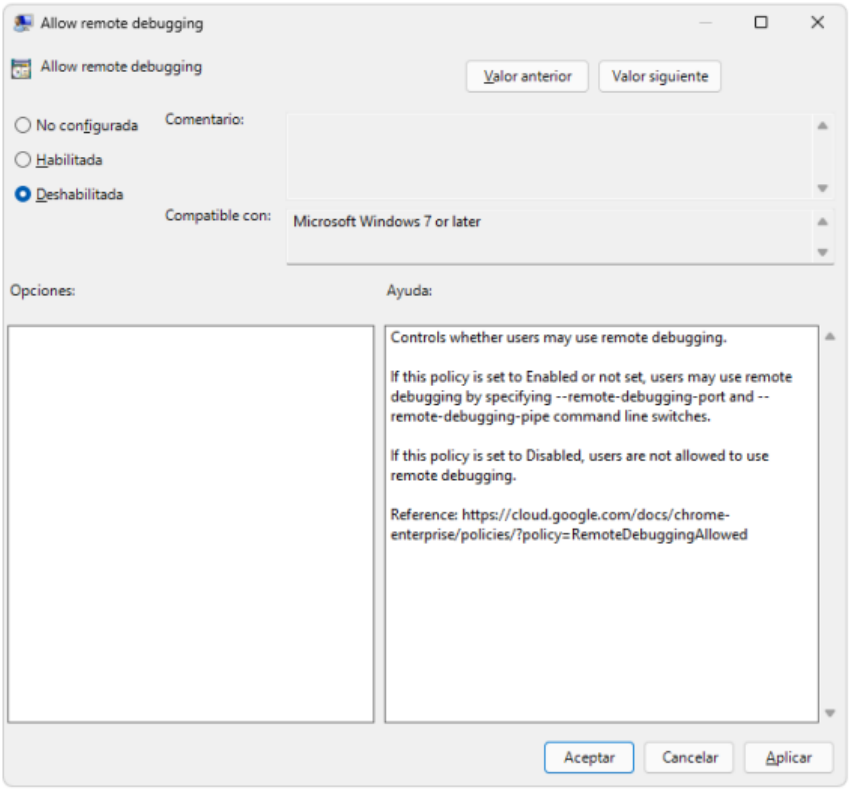
Impacto: Los usuarios no podrán acceder a la función de depuración remota en Google Chrome.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 0.

```
HKEY_LOCAL_MACHINE\Software\Policies\Google\Chrome:RemoteDebuggingAllowed
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Deshabilitada:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\Allow remote debugging
```



3 Privacy

Esta sección contiene recomendaciones que ayudan a mejorar la privacidad del usuario. Las organizaciones deben revisar esta configuración y los posibles impactos para asegurarse de que tengan sentido dentro del entorno, ya que restringen algunas funciones del explorador

3.1 Content settings

3.1.1 (L2) Ensure 'Default cookies setting' is set to 'Enabled: Keep cookies for the duration of the session' (Automated)

Descripción: Al salir de la configuración _RestoreOnStartup _unset da como resultado el uso de _DefaultCookiesSetting _for todos los sitios, si está establecido. Si no _DefaultCookiesSetting _is configurado, se aplica la configuración personal del usuario.

- Deshabilitado (0, se aplica la configuración personal del usuario)
- Permitir que todos los sitios establezcan datos locales (1)

- No permitir que ningún sitio establezca datos locales (2)
- Conservar las cookies durante toda la sesión (4) El estado recomendado para esta configuración es: Habilitado con un valor de Mantener las cookies durante la sesión (4)

NOTA: Si la configuración RestoreOnStartup está configurada para restaurar las direcciones URL de sesiones anteriores, esta configuración no se respetará y las cookies se almacenarán de forma permanente para esos sitios. Un ejemplo de esas direcciones URL son los sitios de inicio de sesión único o de intranet.

Justificación: Las cookies almacenadas permanentemente pueden utilizarse con fines maliciosos.

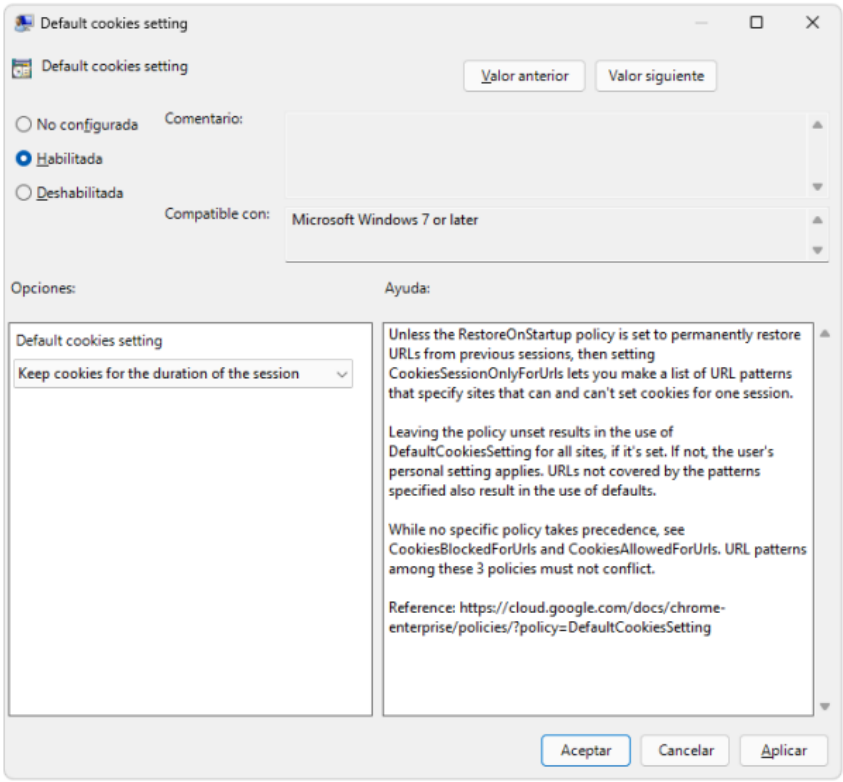
Impacto: Si esta configuración está habilitada, las cookies se borrarán cuando se cierre la sesión.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 4:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:DefaultCookiesSetting
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Habilitada: Conservar las cookies durante la sesión:

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Content
Settings\Default cookies setting
```



3.1.2 (L1) Ensure 'Default geolocation setting' is set to 'Enabled: Do not allow any site to track the users' physical location' (Automated)

Descripción: Google Chrome permite rastrear la ubicación física de un usuario mediante GPS, datos sobre puntos de acceso Wi-Fi cercanos o sitios o torres de señal celular (incluso si no los está usando) y la IP de su computadora.

- Deshabilitado (0, igual que 3)
- Permitir que los sitios rastreen la ubicación física de los usuarios (1)
- No permitir que ningún sitio rastree la ubicación física de los usuarios (2)
- Preguntar cada vez que un sitio quiera rastrear la ubicación física de los usuarios (3) El estado recomendado para esta configuración es: Habilitado con un valor No permitir que ningún sitio rastree la ubicación física de los usuarios (2)

Justificación: Desde el punto de vista de la privacidad, no es deseable presentar indicadores sobre la ubicación del dispositivo, ya que no se puede determinar el procesamiento de esta información. Además, esto puede filtrar información sobre la infraestructura de red alrededor del dispositivo.

Impacto: Si esta opción está inhabilitada, Chrome ya no enviará a Google datos sobre los puntos de acceso Wi-Fi o los sitios o torres de señal de telefonía móvil cercanos

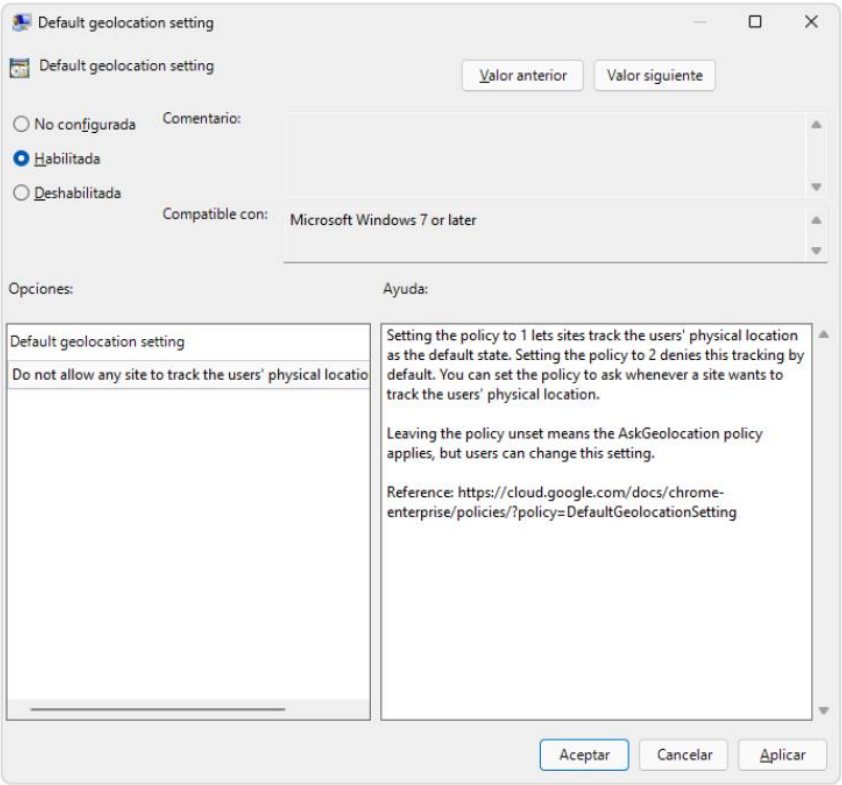
(aunque no los estés usando) ni la dirección IP de tu ordenador. Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección

Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 2:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:DefaultGeolocationSetting
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Habilitada: No permita que ningún sitio realice un seguimiento de la ubicación física de los usuarios:

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Content
Settings\Default geolocation setting
```



3.2 Google Cast

3.2.1 (L1) Ensure 'Enable Google Cast' is set to 'Disabled' (Automated)

Descripción: Google Cast puede enviar el contenido de pestañas, sitios o el escritorio desde el navegador a un sistema de sonido y pantalla remotos. El estado recomendado para esta configuración es: Inhabilitado (0)

Justificación: Google Cast puede enviar el contenido de pestañas, sitios o computadoras de escritorio desde el navegador a dispositivos que no sean de confianza en el segmento de red local.

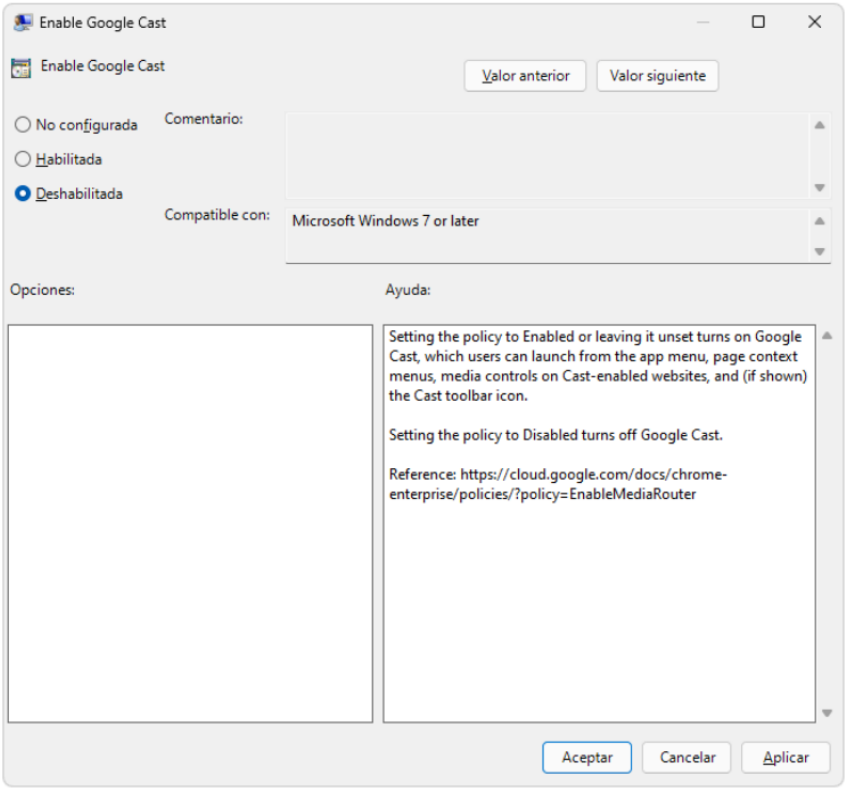
Impacto: Si esta opción está inhabilitada, Google Cast no se activa y no se muestra el icono de la barra de herramientas.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:EnableMediaRouter
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Deshabilitada:

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Google
Cast\Enable Google Cast
```



3.3 (L1) Ensure 'Allow websites to query for available payment methods' is set to 'Disabled' (Automated)

Descripción: esta configuración le permite establecer si un sitio web puede verificar si el usuario tiene métodos de pago guardados. El estado recomendado para esta configuración es: Inhabilitado (0)

Justificación: Guardar información de pago en Google Chrome podría provocar la filtración de datos confidenciales y su uso para fines no legítimos.

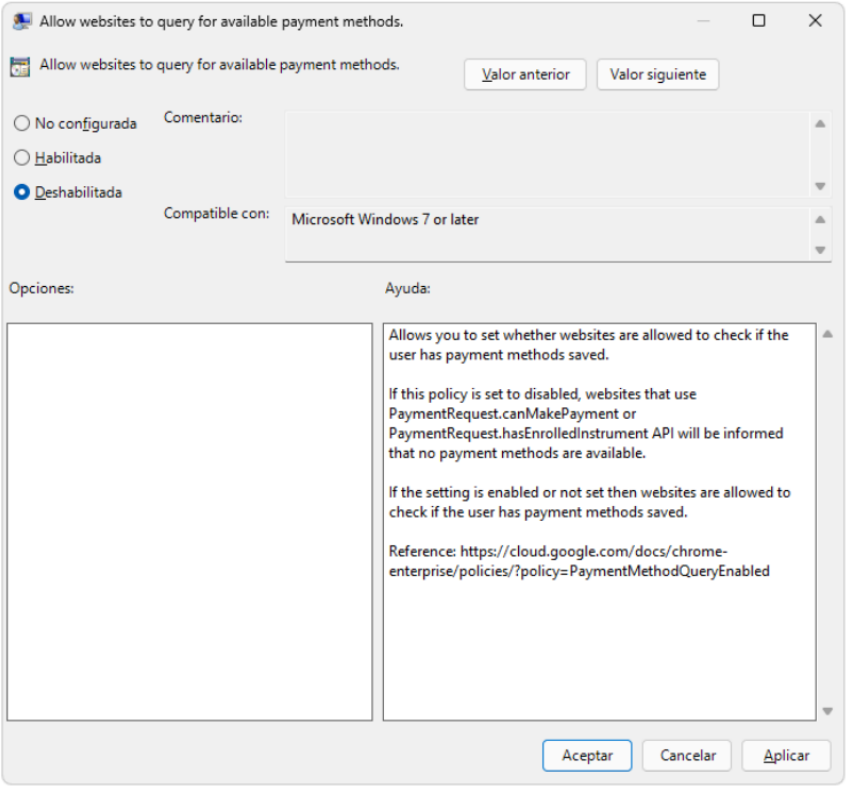
Impacto: Los sitios web no podrán consultar si la información de pago de Google Chrome está disponible.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:PaymentMethodQueryEnabled
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Deshabilitada:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\Allow websites to query for available payment methods.
```



3.4 (L1) Ensure 'Block third party cookies' is set to 'Enabled' (Automated)

Descripción: Chrome permite que las cookies sean configuradas por elementos de la página web que no son del dominio en la barra de direcciones del usuario. Al habilitar esta función, se evita que se establezcan cookies de terceros. El estado recomendado para esta configuración es: Habilitado (1)

Justificación: El bloqueo de las cookies de terceros puede ayudar a proteger la privacidad de un usuario al eliminar una serie de cookies de seguimiento de sitios web. Impacto: Al habilitar esta configuración, se evita que los elementos de la página web que no sean del dominio que se encuentra en la barra de direcciones del explorador establezcan cookies.

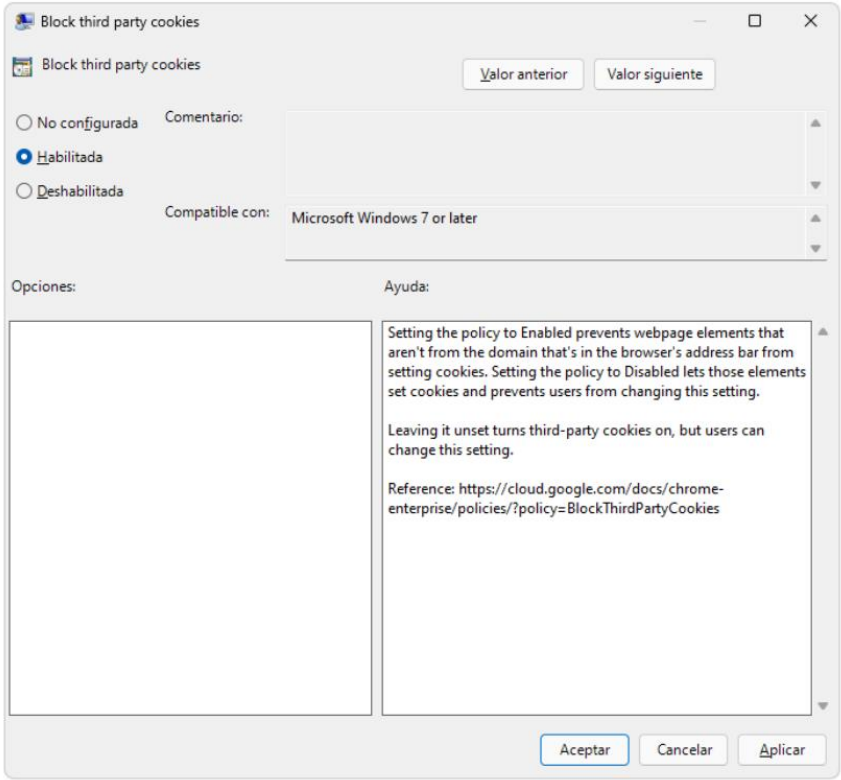
NOTA: Las cookies de terceros y la protección de seguimiento son necesarias para muchos sitios web críticos para la empresa, incluidas las aplicaciones web de Microsoft 365 (Office 365), SalesForce y SAP Analytics Cloud. Si la organización necesita estos servicios u otros, esta configuración se puede deshabilitar.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 1:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:BlockThirdPartyCookies
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Habilitada:

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Block
third party cookies
```



3.5 (L2) Ensure 'Browser sign in settings' is set to 'Enabled: Disabled browser sign-in' (Automated)

Descripción: Google Chrome ofrece la posibilidad de iniciar sesión con tu cuenta de Google y utilizar servicios relacionados con la cuenta, como la sincronización de Chrome. Es posible iniciar sesión en Google Chrome con una cuenta de Google para utilizar servicios como la sincronización, y también se puede utilizar para la configuración y gestión del navegador.

- Deshabilitar el inicio de sesión en el navegador (0)
- Habilitar el inicio de sesión en el navegador (1)
- Obligar a los usuarios a iniciar sesión para usar el navegador (2)

El estado recomendado para esta configuración es: Habilitado con un valor de Deshabilitar el inicio de sesión del explorador (0)

NOTA: Si una organización es cliente de Google Workspace Enterprise, querrá dejar esta configuración habilitada para que los usuarios puedan iniciar sesión con cuentas de Google.

Justificación: Dado que las cuentas externas no están administradas y se utilizan potencialmente para acceder a varios sistemas informáticos privados y a muchos sitios web diferentes, la conexión de cuentas a través del inicio de sesión supone un riesgo de seguridad para la empresa. Interfiere con los mecanismos de gestión corporativa, así como permite una fuga no deseada de información corporativa y una posible mezcla con datos privados ajenos a la empresa.

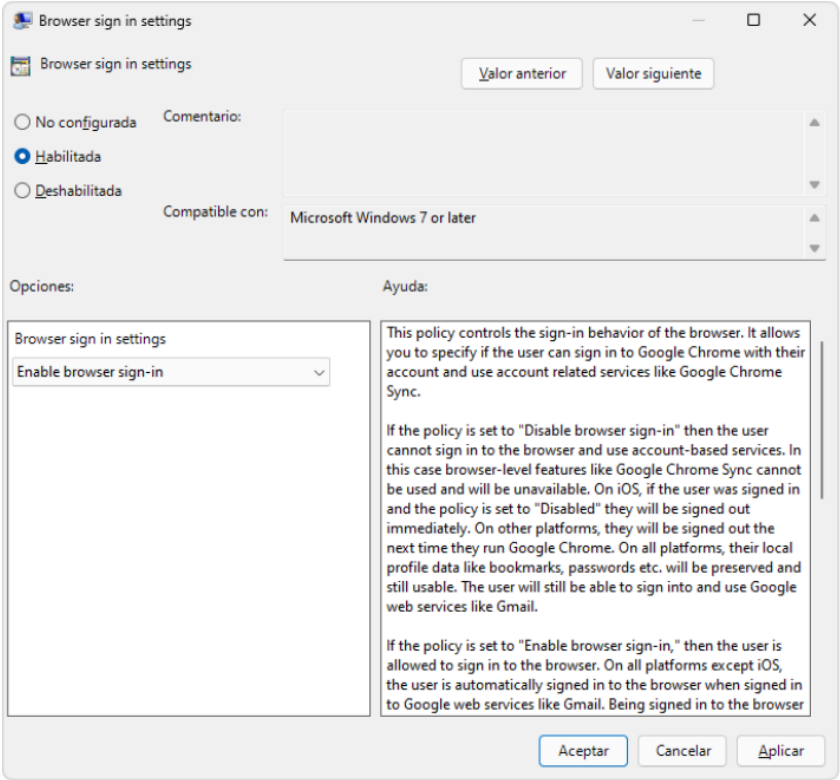
Impacto: Si se configura esta opción, el usuario no puede iniciar sesión en el navegador ni utilizar los servicios basados en cuentas de Google, como la sincronización de Chrome.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:BrowserSignin
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Habilitado: Deshabilitar el inicio de sesión del explorador

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Browser
sign in settings
```



3.6 (L1) Ensure 'Control how Chrome Cleanup reports data to Google' is set to 'Disabled' (Automated)

Descripción: Chrome proporciona una función de limpieza para detectar software no deseado. Si esta configuración está habilitada, los resultados de la limpieza se pueden compartir con Google (según la configuración de SafeBrowsingExtendedReportingEnabled) para ayudar con la detección de software no deseado en el futuro. Estos resultados contendrán metadatos de archivo, extensiones instaladas automáticamente y claves del Registro. Si la configuración está inhabilitada, los resultados de la limpieza no se compartirán con Google, independientemente del valor de SafeBrowsingExtendedReportingEnabled. El estado recomendado para esta configuración es: Deshabilitado (0)

NOTA: Esta configuración no está disponible en instancias de Windows que no están unidas a un dominio de Microsoft® Active Directory®.

Justificación: Los datos anónimos de bloqueo/uso se pueden utilizar para identificar personas, empresas e información, lo que puede considerarse una filtración de datos de los sistemas de la empresa.

Impacto: Chrome Cleanup detectó software no deseado y ya no informará a Google de los metadatos del análisis.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 0:

```
HKEY LOCAL MACHINE\SOFTWARE\Policies\Google\Chrome:ChromeCleanupReportingEnab
led
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Deshabilitada:

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Control
how Chrome Cleanup reports data to Google
```

3.7 (L1) Ensure 'Disable synchronization of data with Google' is set to 'Enabled' (Automated)

Descripción: Google Chrome puede sincronizar los datos del navegador mediante los servicios de sincronización alojados en Google. Algunos ejemplos de datos sincronizados son, entre otros, el historial y los favoritos. El estado recomendado para esta configuración es: Habilitado (1)

NOTA: si su organización permite la sincronización de datos con Google, al inhabilitar esta configuración se sincronizarán las contraseñas guardadas con Google. Justificación: Los datos del navegador no se sincronizarán con Google Cloud.

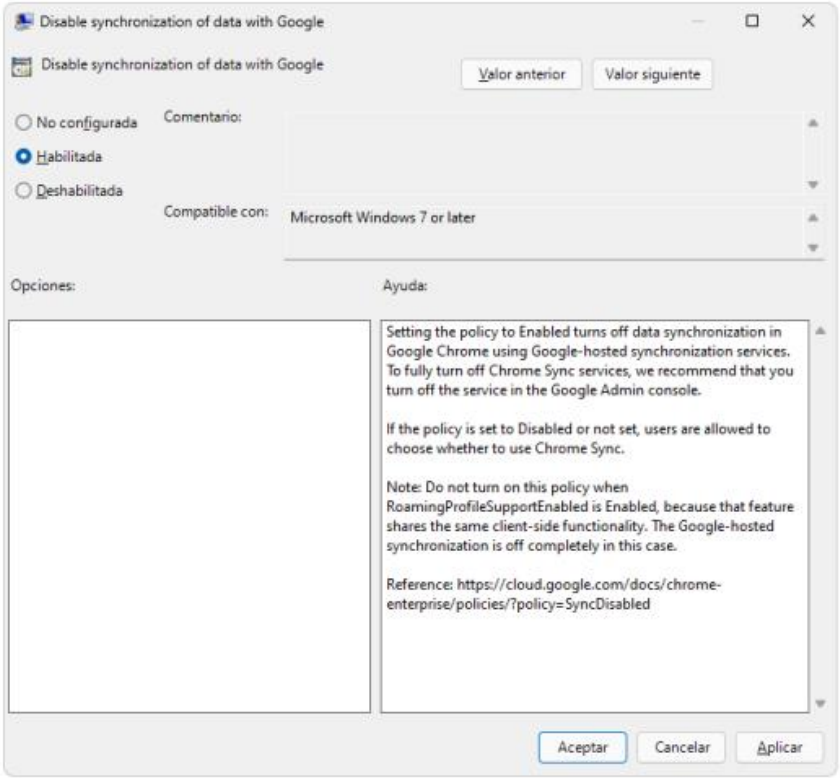
Impacto: Si esta configuración está habilitada, los datos del navegador ya no se sincronizarán con Google en todos los dispositivos o plataformas, lo que permitirá a los usuarios continuar donde lo dejaron.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 1:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:SyncDisabled
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Habilitada:

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Disable
synchronization of data with Google
```



3.8 (L1) Ensure 'Enable alternate error pages' is set to 'Disabled' (Automated)

Descripción: Google Chrome ofrece mostrar sugerencias para la página a la que intentabas acceder cuando no puede conectarse a una dirección web como "Página no encontrada". El estado recomendado para esta configuración es: Deshabilitado (0)

Justificación: El uso de sugerencias de navegación puede filtrar información sobre el sitio web que se va a visitar.

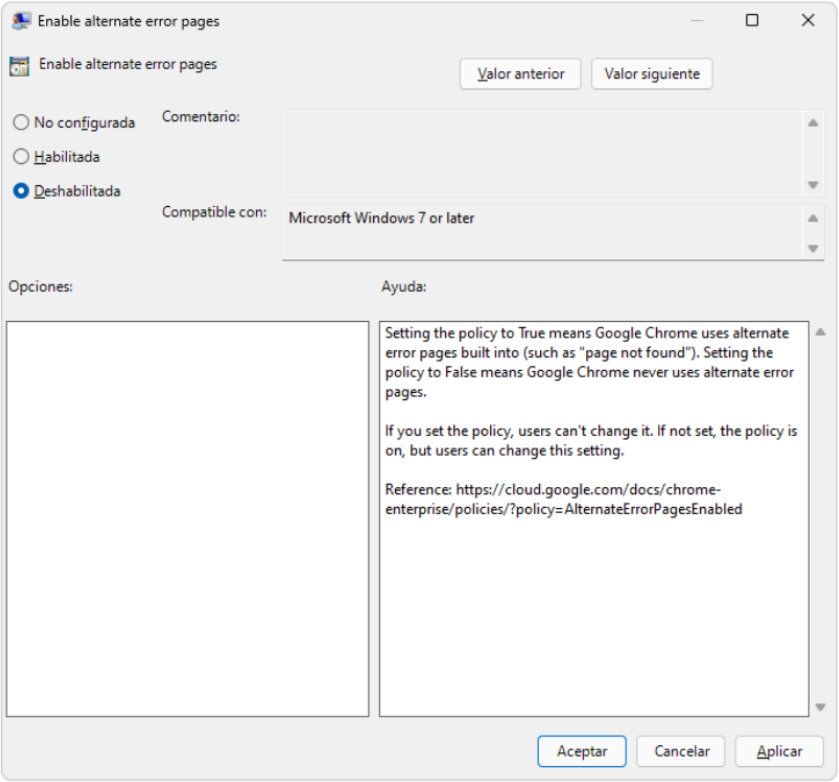
Impacto: Si esta configuración está inhabilitada, Chrome ya no usará un servicio web para ayudar a resolver errores de navegación.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:AlternateErrorPagesEnabled
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Deshabilitada:

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Enable
alternate error pages
```



3.9 (L1) Ensure 'Enable deleting browser and download history' is set to 'Disabled' (Automated)

Descripción: Google Chrome puede eliminar el navegador y el historial de descargas mediante el menú de borrado de datos de navegación. El estado recomendado para esta configuración es: Deshabilitado (0)

NOTA: Incluso cuando esta configuración está deshabilitada, no se garantiza que se conserve el historial de navegación y descargas. Los usuarios pueden editar o eliminar directamente los archivos de la base de datos del historial, y el propio navegador puede eliminar (en función del período de caducidad) o archivar cualquiera o todos los elementos del historial en cualquier momento

Justificación: Si los usuarios pueden eliminar los sitios web que han visitado o los archivos que han descargado, les resultará más fácil ocultar las pruebas de que han visitado sitios no autorizados o maliciosos.

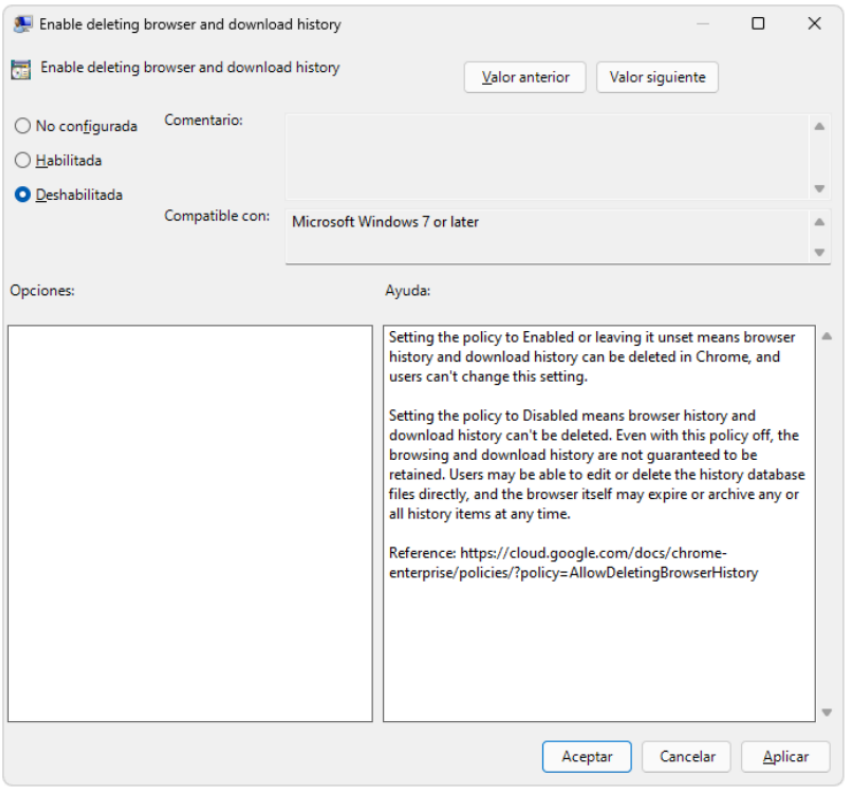
Impacto: Si esta configuración está desactivada, el historial de navegación y descarga no se puede eliminar mediante el menú Borrar datos de navegación.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:AllowDeletingBrowserHistor
y
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Deshabilitada:

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Enable
deleting browser and download history
```



3.10 (L1) Ensure 'Enable predict network actions` is set to 'Enabled: Do not predict actions on any network connection' (Automated)

Descripción: Google Chrome viene con la función de predicción de red que proporciona precarga de DNS, preconexión TCP y SSL, y representación previa de páginas web.

- Predecir las acciones de red en cualquier conexión de red (0) o (1)

- No predecir las acciones de red en ninguna conexión de red (2) El estado recomendado para esta configuración es: Habilitado con un valor de No predecir acciones de red en ninguna conexión de red (2)

Justificación: La apertura de conexiones a recursos que no se pueden utilizar podría permitir conexiones innecesarias que aumenten la superficie de ataque y, en algunos casos, podría provocar la apertura de conexiones a recursos que el usuario no ha utilizado tienen la intención de utilizar.

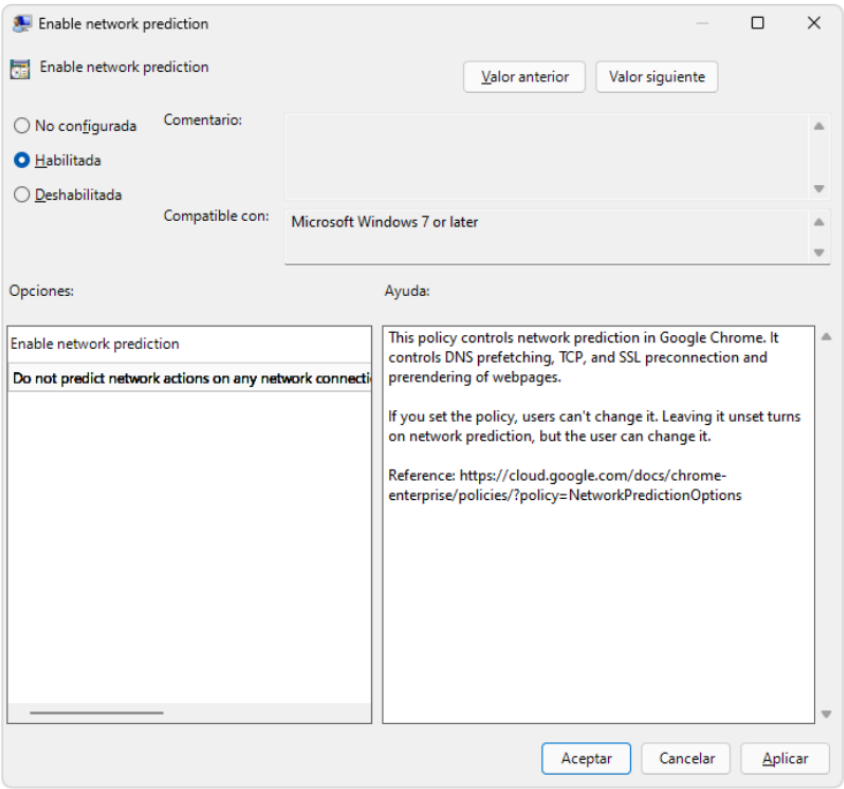
Impacto: a los usuarios no se les presentarán predicciones de páginas web.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 2:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:NetworkPredictionOptions
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Habilitada: No predecir acciones de red en ninguna conexión de red:

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Enable
network prediction
```



3.11 (L1) Ensure 'Enable or disable spell checking web service' is set to 'Disabled' (Automated)

Descripción: Google Chrome puede utilizar el servicio web de Google para ayudar a resolver errores ortográficos. El estado recomendado para esta configuración es: Deshabilitado (0)

Justificación: La información introducida puede filtrarse al servicio web de revisión ortográfica de Google.

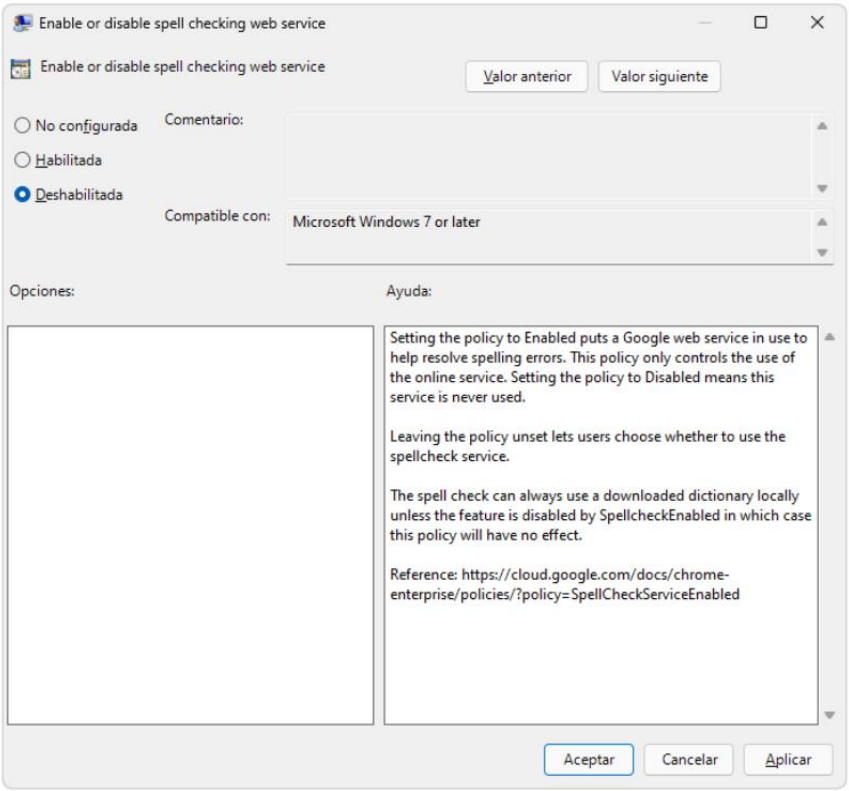
Impacto: Después de inhabilitar esta función, Chrome ya no envía todo el contenido de los campos de texto a Google a medida que los escribes. La revisión ortográfica aún se puede realizar usando un diccionario descargado. Esta configuración solo controla el uso del servicio en línea.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:SpellCheckServiceEnabled
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Deshabilitada:

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Enable
or disable spell checking web service
```



3.12 (L1) Ensure 'Enable reporting of usage and crash-related data' is set to 'Disabled' (Automated)

Descripción: esta configuración controla los informes anónimos de datos relacionados con el uso y los bloqueos de Google Chrome a Google. El estado recomendado para esta configuración es: Deshabilitado (0)

NOTA: Esta configuración no está disponible en instancias de Windows que no están unidas a un dominio de Microsoft® Active Directory®.

Justificación: Los datos anónimos de bloqueo/uso se pueden utilizar para identificar personas, empresas e información, lo que puede considerarse datos ex-filtración de los sistemas de la empresa.

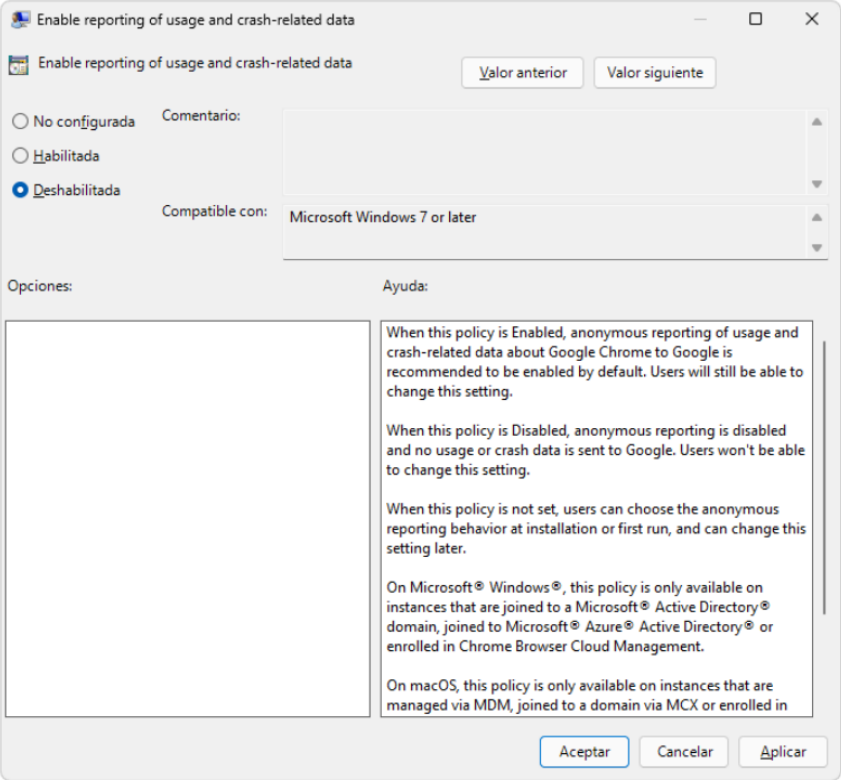
Impacto: Si esta configuración está inhabilitada, esta información no se envía a Google.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:MetricsReportingEnabled
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Deshabilitada:

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Enable
reporting of usage and crash-related data
```



3.13 (L1) Ensure 'Enable Safe Browsing for trusted sources' is set to 'Disabled' (Automated)

Descripción: Google Chrome se puede ajustar para permitir descargas sin comprobaciones de Navegación segura cuando el archivo solicitado procede de una fuente de confianza. Las fuentes de confianza se pueden definir mediante la recomendación "Configurar la lista de dominios en los que la Navegación segura no activará advertencias". El estado recomendado para esta configuración es: Deshabilitado (0)

NOTA: En Microsoft® Windows®, esta funcionalidad solo está disponible en instancias que están unidas a un dominio de Microsoft® Active Directory®, que se ejecutan en Windows 10 Pro o que están inscritas en Administración en la nube del navegador Chrome.

Justificación: La información solicitada de fuentes confiables no se enviará a los servidores de navegación segura de Google.

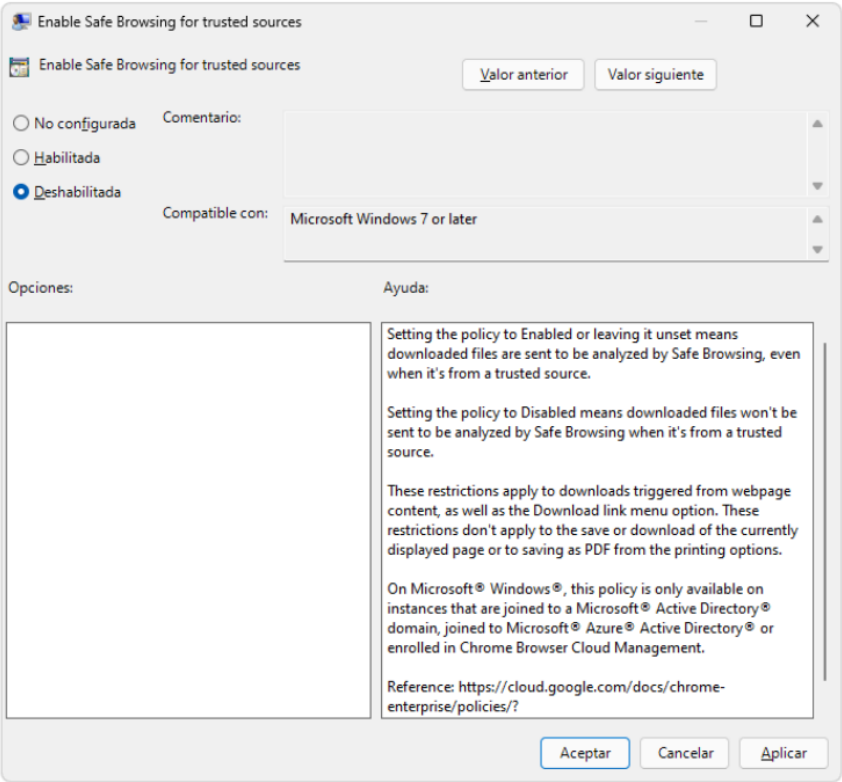
Impacto: Si esta configuración está inhabilitada, los servicios de Google no comprobarán los archivos descargados de los recursos de la intranet.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 0

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:SafeBrowsingForTrustedSour
cesEnabled
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Deshabilitada:

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Enable
Safe Browsing for trusted sources
```



3.14 (L2) Ensure 'Enable search suggestions' is set to 'Disabled' (Automated)

Descripción: Google Chrome ofrece sugerencias en el cuadro multifunción de Google Chrome mientras el usuario escribe. El estado recomendado para esta configuración es: Deshabilitado (0)

Justificación: El uso de sugerencias de búsqueda puede filtrar información tan pronto como se escribe/pega en el cuadro multifunción, por ejemplo, contraseñas, servicios web internos, estructuras de carpetas, etc.

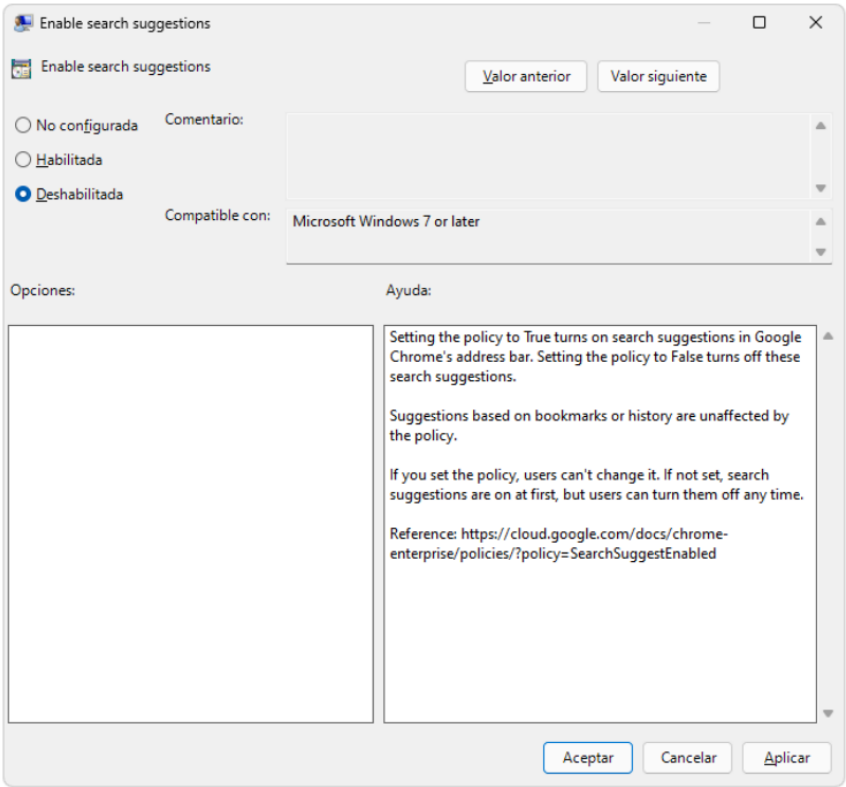
Impacto: El usuario tiene que enviar la solicitud de búsqueda de forma activa utilizando el botón de búsqueda o pulsando "Intro".

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:SearchSuggestEnabled
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Deshabilitada:

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Enable
search suggestions
```



3.15 (L2) Ensure 'Enable Translate' is set to 'Disabled' (Automated)

Descripción: esta configuración habilita los servicios de traducción de Google en Google Chrome. El estado recomendado para esta configuración es: Deshabilitado (0)

Justificación: Es posible que el contenido de las páginas web internas se filtre al servicio de traducción de Google.

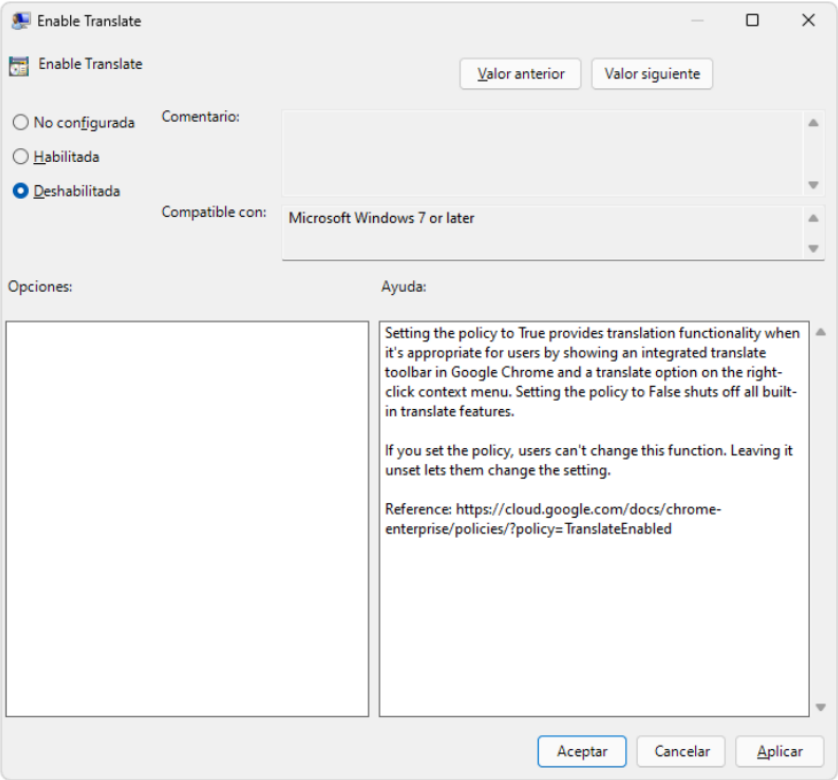
Impacto: Después de inhabilitar esta función, el contenido de una página web ya no se envía a Google para su traducción.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:TranslateEnabled
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Deshabilitada:

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Enable
Translate
```



3.16 (L1) Ensure 'Enable URL-keyed anonymized data collection' is set to 'Disabled' (Automated)

Descripción: Google Chrome ofrece la función de recopilación de datos anonimizados con clave de URL. Esto envía las URL de las páginas que visita el usuario a Google para optimizar sus servicios. El estado recomendado para esta configuración es: Inhabilitado (0)

Justificación: Se debe inhabilitar la recopilación de datos anonimizados, ya que no está claro qué información se envía exactamente a Google.

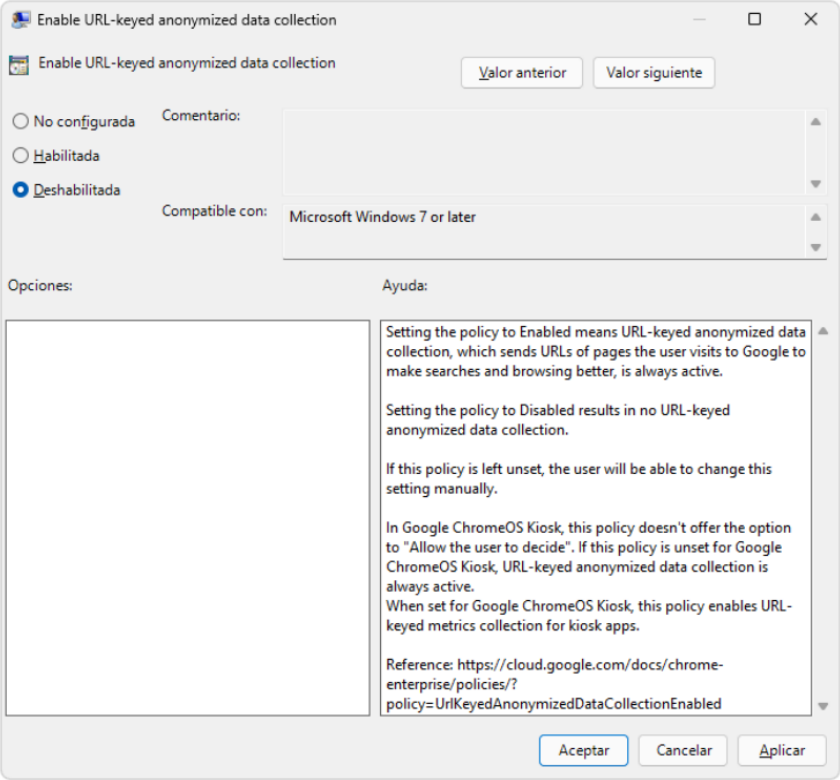
Impacto: No se enviarán datos anonimizados a Google para ayudar a optimizar sus servicios.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:UrlKeyedAnonymizedDataColl
ectionEnabled
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Deshabilitada:

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Enable
URL-keyed anonymized data collection
```



4 Data Loss Prevention

Esta sección contiene recomendaciones para ayudar a prevenir y proteger contra la pérdida no deseada de datos. Las organizaciones deben revisar esta configuración y los posibles impactos para asegurarse de que tienen sentido dentro del entorno, ya que restringen algunas funciones del explorador.

4.1 Allow or deny screen capture

4.1.1 (L2) Ensure 'Allow or deny screen capture' is set to 'Disabled' (Automated)

Descripción: esta configuración controla si Google Chrome puede usar las API para compartir pantalla, incluidas las reuniones en línea basadas en la web, el video o el uso

compartido de pantalla. El estado recomendado para esta configuración es: Deshabilitado (0)

NOTA: Esta configuración no se tiene en cuenta (y un sitio podrá usar API de uso compartido de pantalla) si el sitio coincide con un patrón de origen en cualquiera de las siguientes configuraciones: ScreenCaptureAllowedByOrigins, WindowCaptureAllowedByOrigins, TabCaptureAllowedByOrigins, SameOriginTabCaptureAllowedByOrigins.

Justificación: Permitir las API de pantalla compartida dentro de Google Chrome podría permitir que se compartan datos confidenciales a través de capturas de pantalla.

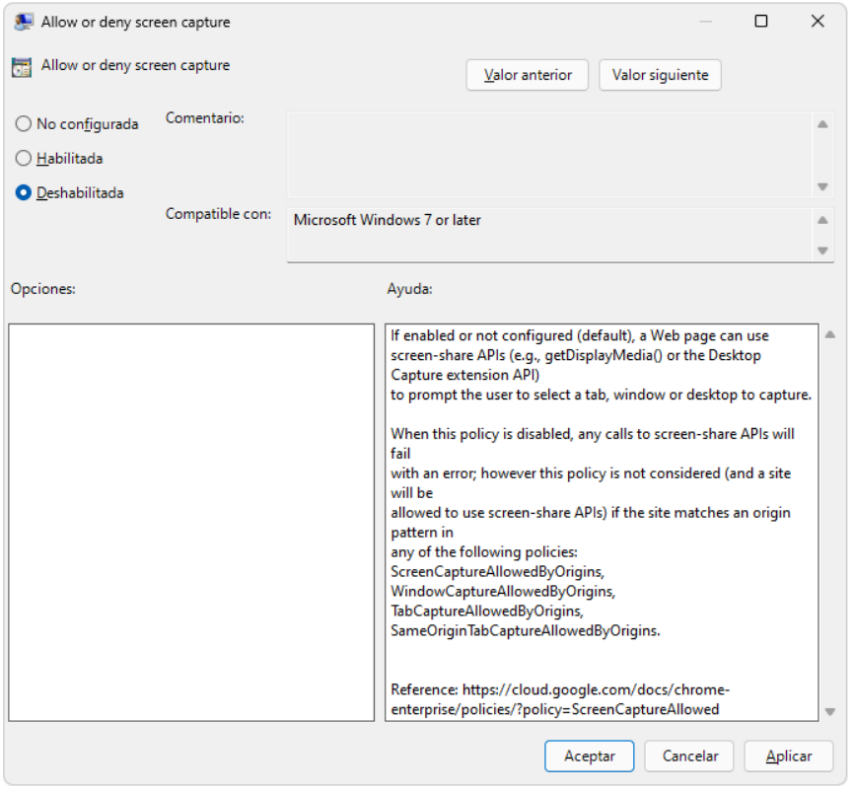
Impacto: los usuarios no podrán utilizar las API que admiten reuniones basadas en web (videoconferencia, uso compartido de pantalla), vídeo y captura de pantalla. Esto podría causar interrupciones a los usuarios que pueden haber utilizado estas capacidades en el pasado.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:ScreenCaptureAllowed
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Deshabilitada:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\Allow or deny screen capture\Allow or deny screen capture
```



4.2 Content settings

4.2.1 (L2) Ensure 'Control use of the Serial API' is set to 'Enabled: Do not allow any site to request access to serial ports via the Serial API' (Automated)

Descripción: esta configuración controla el acceso al sitio web y el uso del puerto serie del sistema.

- No permita que ningún sitio solicite acceso a los puertos serie a través de la API serie (2)
- Permitir que los sitios soliciten al usuario que conceda acceso a un puerto serie (3)

El estado recomendado para esta configuración es: No permita que ningún sitio solicite acceso a los puertos serie a través de la API serie (2)

NOTA: Si se necesita un control más granular (por sitio web), esta configuración se puede usar en combinación con SerialAllowAllPortsForUrls, Configuración de SerialAskForUrls y SerialBlockedForUrls. Por ejemplo, SerialAllowAllPortsForUrls se puede usar para permitir el acceso del puerto serie a sitios específicos. Consulte las referencias a continuación para obtener más información.

Justificación: Impedir el acceso a los puertos serie del sistema puede impedir que los sitios malintencionados utilicen estos puertos y accedan a los dispositivos conectados.

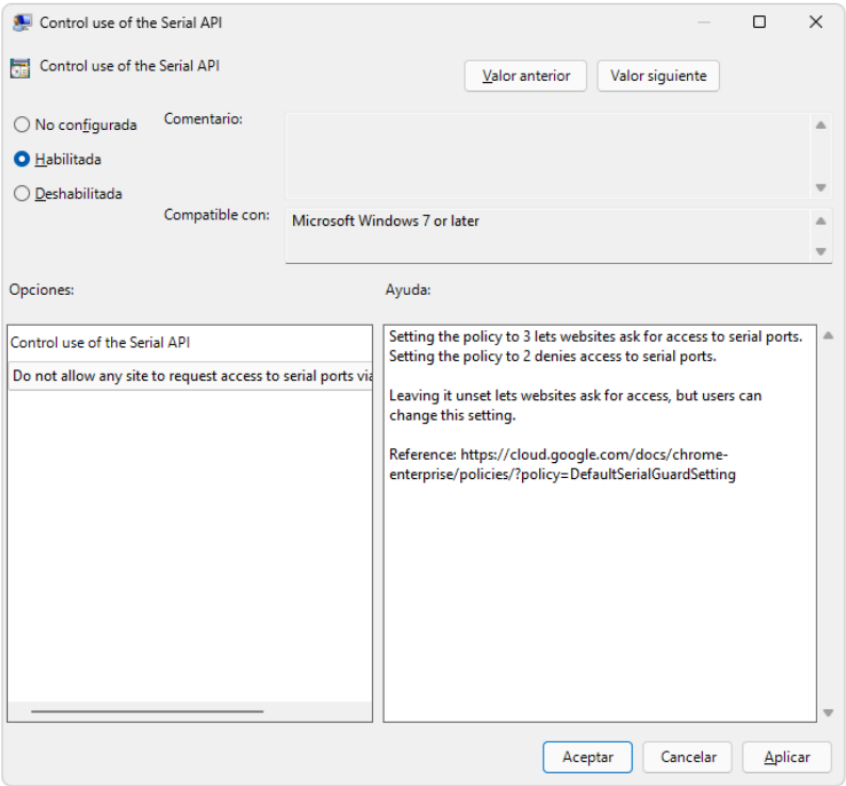
Impacto: esta configuración también impediría que los sitios legítimos accedieran a ella.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 2:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:DefaultSerialGuardSetting
```

Corrección: Para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Habilitada: No permita que ningún sitio solicite acceso a los puertos serie a través de la API serie:

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Content
settings\Control use of the Serial API
```



4.2.2 (L2) Ensure 'Default Sensors Setting' is set to 'Enabled: Do not allow any site to access sensors' (Automated)

Descripción: esta configuración controla el acceso al sitio web y el uso de los sensores del sistema, como el movimiento y la luz.

- Permitir que los sitios accedan a los sensores (1)
- No permita que ningún sitio acceda a los sensores (2)

El estado recomendado para esta configuración es: No permitir que ningún sitio acceda a los sensores (2) El estado recomendado para esta configuración es: Habilitado con un valor de No permitir que ningún sitio acceda a los sensores

NOTA: Si se necesita un control más granular (por sitio web), esta configuración se puede usar en combinación con la configuración de SensorsAllowedForUrls y SensorsBlockedForUrls. Por ejemplo, SensorsAllowedForUrls se puede usar para permitir el acceso de sensores a sitios específicos. Consulte las referencias a continuación para obtener más información.

Justificación: Impedir el acceso a los sensores del sistema puede impedir que los sitios malintencionados utilicen estos sensores para la creación de perfiles de usuario (OpSec).

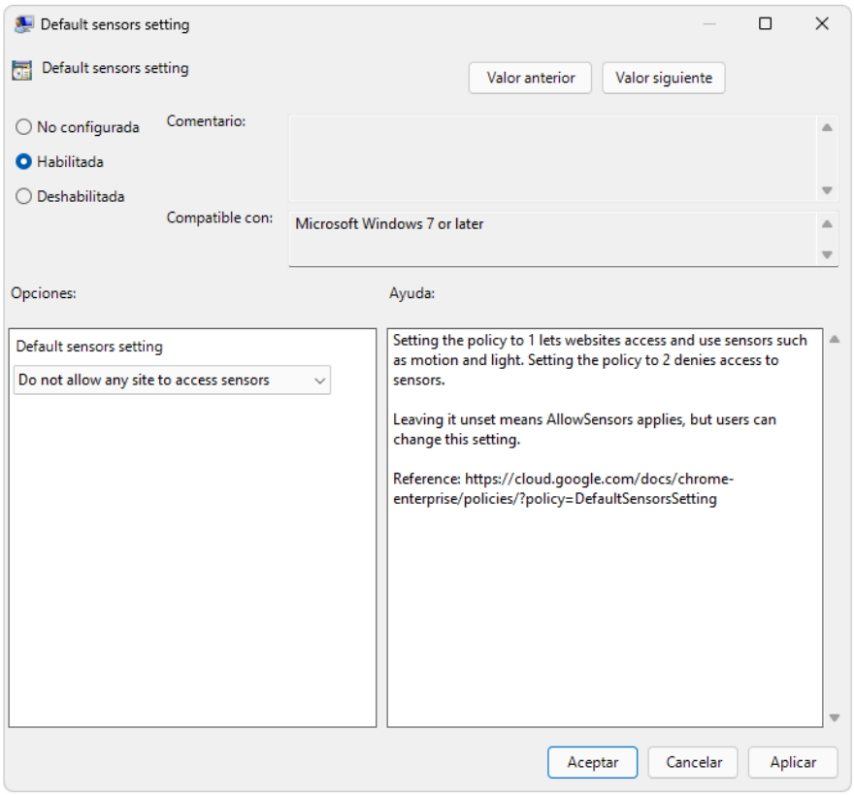
Impacto: esta configuración también impediría que los sitios legítimos accedieran a ella.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 2:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:DefaultSensorsSetting
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Habilitada: No permita que ningún sitio acceda a los sensores:

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Content
settings\Default sensors setting
```



4.2.3 (L1) Ensure 'Allow clipboard for these sites' Is Configured (Manual)

Descripción: esta configuración permite a los administradores enumerar sitios específicos que tienen acceso a los permisos del sitio del portapapeles.

Nota: Esto no incluye el uso de atajos de teclado. Esos no están bloqueados por el permiso del sitio del portapapeles.

Justificación: La configuración de esta directiva permite que las direcciones URL especificadas tengan acceso a los permisos del sitio del portapapeles. Esto permitirá que los sitios especificados tengan acceso a datos en el portapapeles que otros sitios no tienen. Se recomienda establecer DefaultClipboardSetting en deshabilitado, por lo que esta lista sería la única que tendría acceso a los datos del portapapeles.

Impacto: la aplicación de esta recomendación puede hacer que la funcionalidad del portapapeles no funcione de forma idéntica para todos los sitios.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse individualmente en las direcciones URL permitidas de la organización:

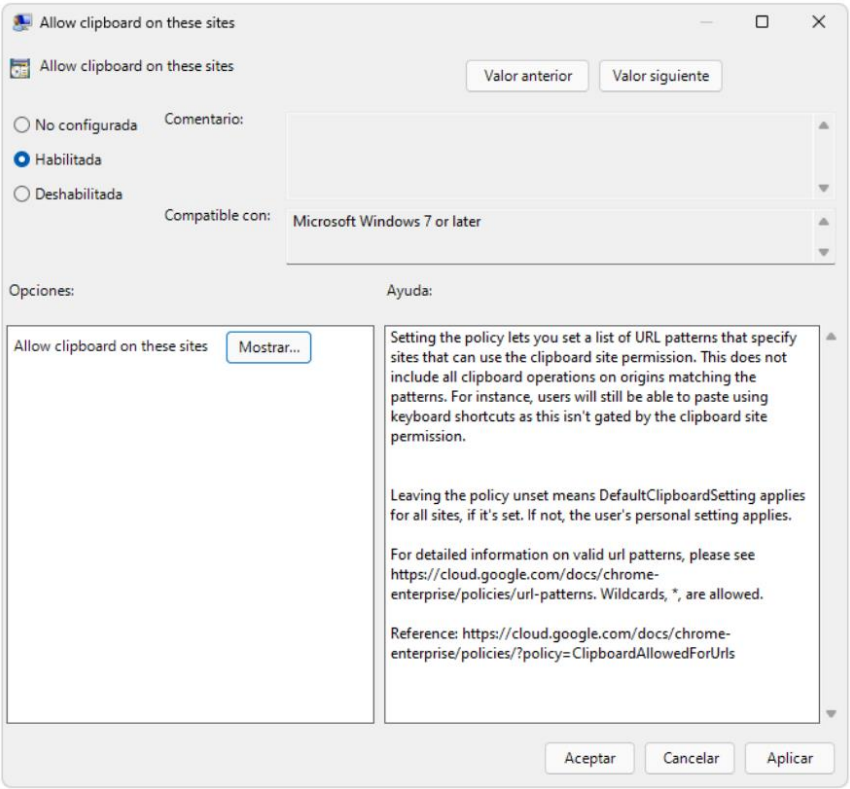
```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\ClipboardAllowedForUrls\<n
umber> = <url>
```

Example:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\ClipboardAllowedForUrls\1
= https://www.example.com
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\ClipboardAllowedForUrls\2
= [*.]example.edu
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\ClipboardAllowedForUrls\3
= https://www.example.net
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Habilitada y establezca Mostrar en las direcciones URL aprobadas:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\Content settings\Allow clipboard on these sites
```



4.2.4 (L1) Ensure 'Block clipboard on these sites' Is Configured (Manual)

Descripción: esta configuración permite a los administradores enumerar sitios específicos que no tienen acceso a los permisos del sitio del portapapeles.

Nota: Esto no incluye el uso de atajos de teclado. Esos no están bloqueados por el permiso del sitio del portapapeles.

Justificación: La especificación de direcciones URL que no tienen acceso a los permisos del sitio del portapapeles limita los datos de los sitios que tienen acceso a los datos del portapapeles y permite que más sitios tengan acceso. Al establecer esta directiva, se deniega a las direcciones URL especificadas el acceso a los permisos del sitio del portapapeles. Esto limitará los sitios especificados para acceder a los datos del portapapeles que otros sitios tienen. Se recomienda establecer DefaultClipboardSetting en deshabilitado, por lo que esta lista sería una copia de seguridad de esa directiva en caso de que se habilitara, se dejara como predeterminada o se quitara. Impacto: la aplicación de esta recomendación puede hacer que la funcionalidad del portapapeles no funcione de forma idéntica para todos los sitios.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse individualmente en las direcciones URL bloqueadas de su organización

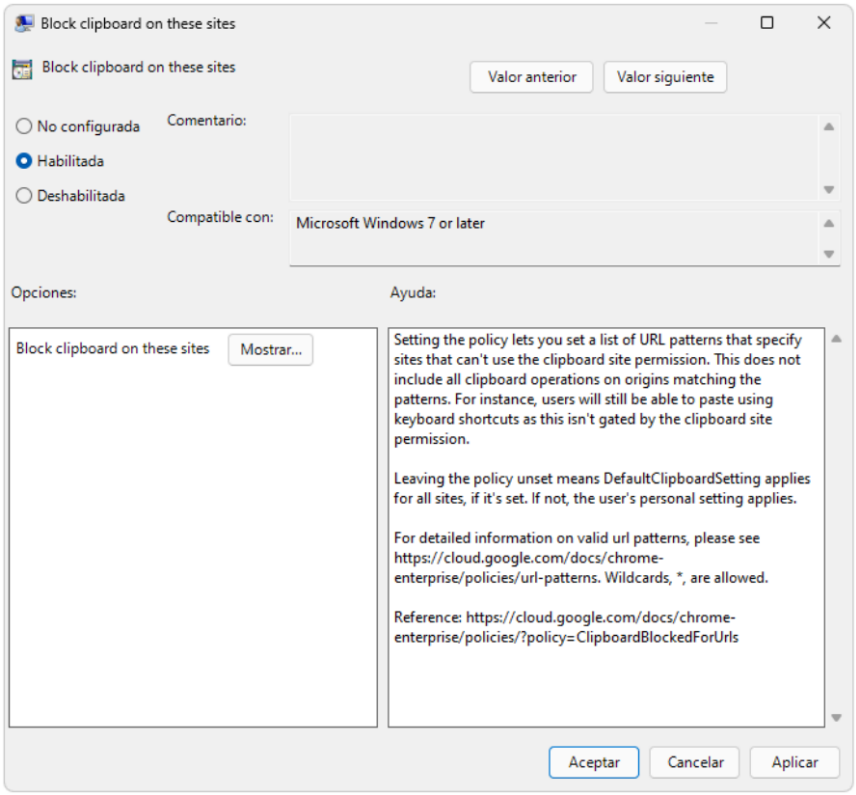
```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\ClipboardBlockedForUrls\<n
umber> = <url>
```

Example:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\ClipboardBlockedForUrls\1
= https://www.example.com
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\ClipboardBlockedForUrls\2
= [*.]example.edu
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\ClipboardBlockedForUrls3 =
https://www.example.net
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Habilitada y establezca Mostrar en las direcciones URL bloqueadas:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\Content settings\Block clipboard on these sites
```



4.2.5 (L1) Ensure 'Default clipboard setting' Is 'Enabled' to 'Deny Permissions' (Automated)

Descripción: esta configuración controla los valores predeterminados para el acceso a los permisos del portapapeles desde los sitios. Se puede configurar para:

- Deshabilitado (2): no permite el acceso al permiso del sitio del portapapeles por parte de ningún sitio
- Habilitado (3): los sitios piden al usuario que permita el acceso al permiso del sitio del portapapeles Si el valor de DefaultClipboardSetting no se cambia del valor predeterminado, se comportará como si estuviera habilitado. ClipboardAllowedForUrls o ClipboardBlockedForUrls invalidarán esta configuración para cualquier sitio que coincida con los patrones de URL configurados.

Con la configuración deshabilitada, las organizaciones deberán establecer ClipboardAllowedForUrls para las direcciones URL que deseen exentar.

Justificación: El portapapeles almacena datos, texto e imágenes que se comparten entre todas las aplicaciones. Una organización deshabilitaría el acceso al portapapeles para impedir que los sitios lean el contenido del portapapeles durante la visita.

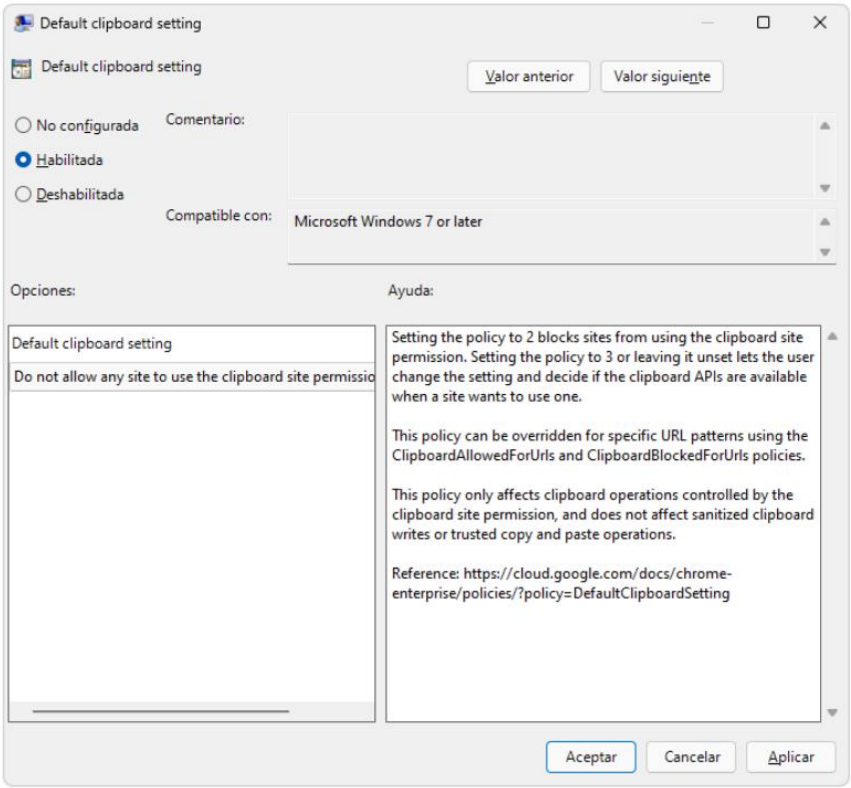
Impacto: No permitir que los sitios tengan acceso al permiso del portapapeles puede causar problemas con el formato o el acceso a las imágenes necesarias en el portapapeles.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 2:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:DefaultClipboardSetting
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Habilitada: No permita que ningún sitio use el permiso de sitio del portapapeles:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\Content settings\Default clipboard setting
```



4.2.6 (L2) Ensure 'Default Window Management permissions setting' Is 'Enabled' to 'Deny Permission' (Automated)

Descripción: esta configuración puede denegar automáticamente el acceso a los permisos de administración de ventanas por parte de los sitios. Se puede configurar para:

• Deshabilitado (2): No permite el acceso al permiso de administración de ventanas por parte de ningún sitio

• Habilitado (3): Un sitio debe preguntar al usuario cada vez que desee acceder al permiso de administración de ventanas.

Si el valor de DefaultWindowManagementSetting no se cambia con respecto al valor predeterminado, se comportará como si estuviera habilitado. WindowManagementAllowedForUrls o WindowManagementBlockedForUrls invalidarán esta configuración para cualquier sitio que coincida con los patrones de URL configurados.

Justificación: Denegar el acceso a la Administración de ventanas puede impedir que los sitios fraudulentos abran ventanas adicionales del navegador. Al bloquear las ventanas adicionales, una organización podría evitar que se abran instancias de sitios nefastos en ubicaciones de las que el usuario no es consciente.

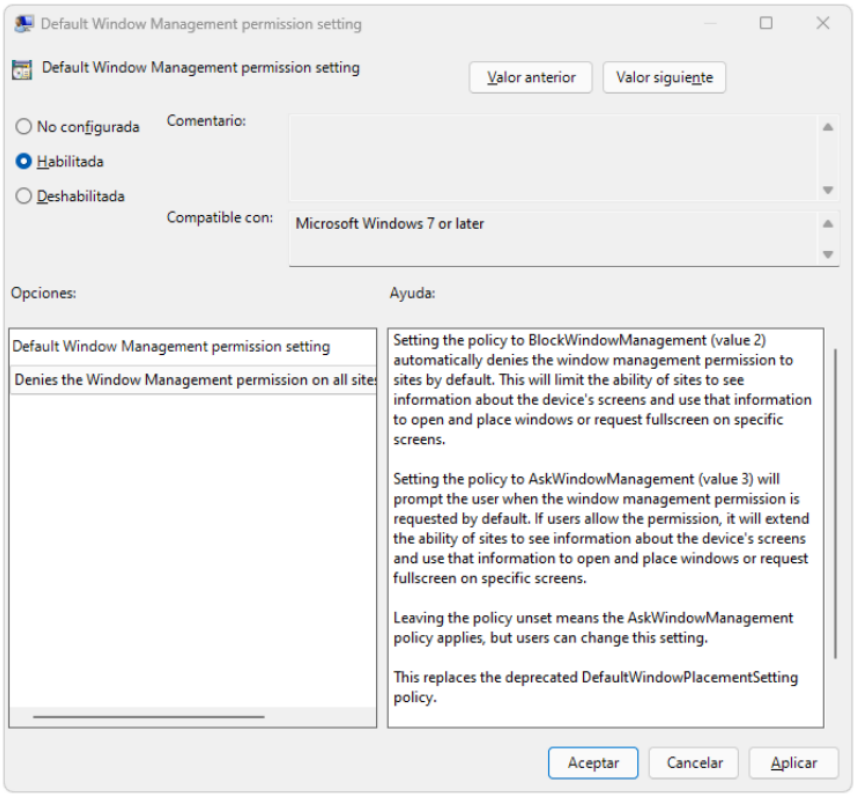
Impacto: si se deshabilita esta opción, se eliminaría la funcionalidad del usuario para decidir qué sitios tienen acceso al permiso Administración de ventanas, lo que podría afectar a las direcciones URL necesarias de la organización.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 2:

```
HKEY LOCAL MACHINE\SOFTWARE\Policies\Google\Chrome:DefaultWindowManagementSet
ting
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Habilitado y deniega el permiso Administración de ventanas en todos los sitios de forma predeterminada:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\Content settings\Default Window Management permission setting
```



4.2.7 (L2) Ensure 'Allow Window Management permission on these sites' Is Configured (Manual)

Descripción: esta configuración puede permitir automáticamente el acceso a los permisos de administración de ventanas para sitios específicos. Si el valor de WindowManagementAllowedForUrls no se cambia con respecto al valor predeterminado, seguirá la configuración de DefaultWindowManagementSetting.

Justificación: Permitir que solo sitios específicos tengan acceso a la Administración de ventanas solo permitirá que los sitios permitidos vean información sobre las pantallas del dispositivo, abran ventanas adicionales del navegador que especifiquen la ubicación y el tamaño de la ventana.

Impacto: la aplicación de esta recomendación puede hacer que los sitios visitados no se muestren según lo previsto.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse individualmente en las direcciones URL permitidas de la organización:

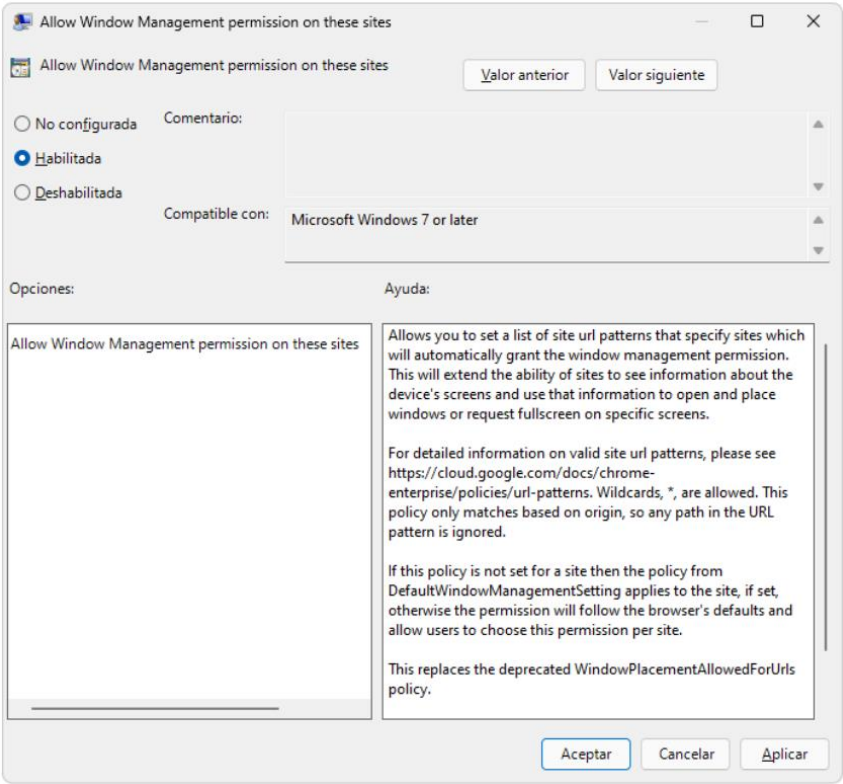
```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\WindowManagementAllowedFor
Urls\<number> = <url>
```

Example:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\WindowManagementAllowedFor
Urls\1 = https://www.example.com
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\WindowManagementAllowedFor
Urls\2 = [*.]example.edu
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\WindowManagementAllowedFor
Urls\3 = https://www.example.net
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Habilitada y establezca Mostrar en las direcciones URL aprobadas:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\Content settings\Allow Window Management permission on these sites
```



4.2.8 (L2) Ensure 'Block Window Management permission on these sites' Is Configured (Manual)

Descripción: esta configuración puede denegar automáticamente el acceso a los permisos de administración de ventanas para sitios específicos. Se puede configurar para: Si el valor de WindowManagementBlockedForUrls no se cambia con respecto al valor predeterminado, seguirá la configuración de DefaultWindowManagementSetting.

Justificación: La especificación de direcciones URL que no tienen acceso a los permisos de administración de ventanas limita los datos de los sitios que tienen acceso a los datos del portapapeles y permite que más sitios tengan acceso.

Impacto: la aplicación de esta recomendación puede hacer que los sitios visitados no se muestren según lo previsto.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse individualmente en las direcciones URL permitidas de la organización:

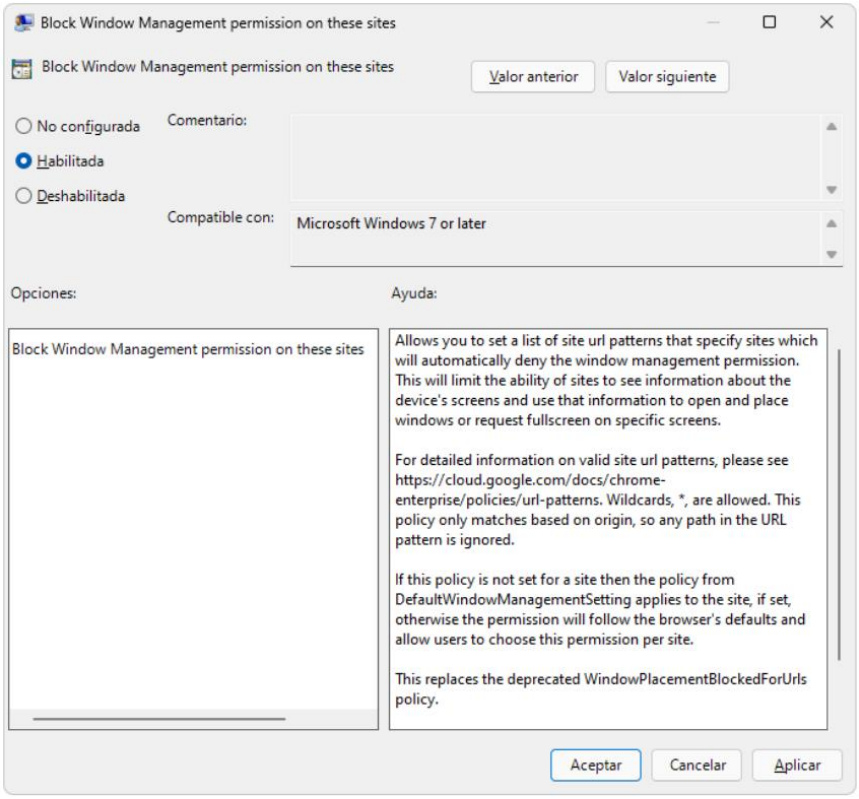
```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\WindowManagementBlockedFor
Urls\<number> = <url>
```

Example:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\WindowManagementBlockedFor
Urls\1 = https://www.example.com
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\WindowManagementBlockedFor
Urls\2 = [*.]example.edu
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\WindowManagementBlockedFor
Urls\3 = https://www.example.net
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Habilitada y establezca Mostrar en las direcciones URL bloqueadas:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\Content settings\Block Window Management permission on these sites
```



4.3 (L2) Ensure 'Allow invocation of file selection dialogs' is set to 'Disabled' (Automated)

Descripción: esta configuración permite el acceso a los archivos locales mediante los diálogos de selección de archivos en Google Chrome. El estado recomendado para esta configuración es: Deshabilitado (0)

Justificación: Permitir que los usuarios importen favoritos, carguen archivos y guarden vínculos podría plantear posibles riesgos de seguridad al permitir que los datos se carguen en sitios externos o al descargar archivos malintencionados. Al no permitir el cuadro de diálogo de selección de archivos, no se solicitará al usuario final que realice cargas/descargas, lo que evita la exfiltración de datos y la posible infección del sistema por malware.

Impacto: Si deshabilita esta configuración, ya no se preguntará a los usuarios cuando realicen acciones que activen un cuadro de diálogo de selección de archivos. En su lugar, el cuadro de diálogo de selección de archivos asume que el usuario hizo clic en "Cancelar". Al no ser este el comportamiento por defecto, el impacto en el usuario será notable, y el usuario no podrá subir y descargar archivos.

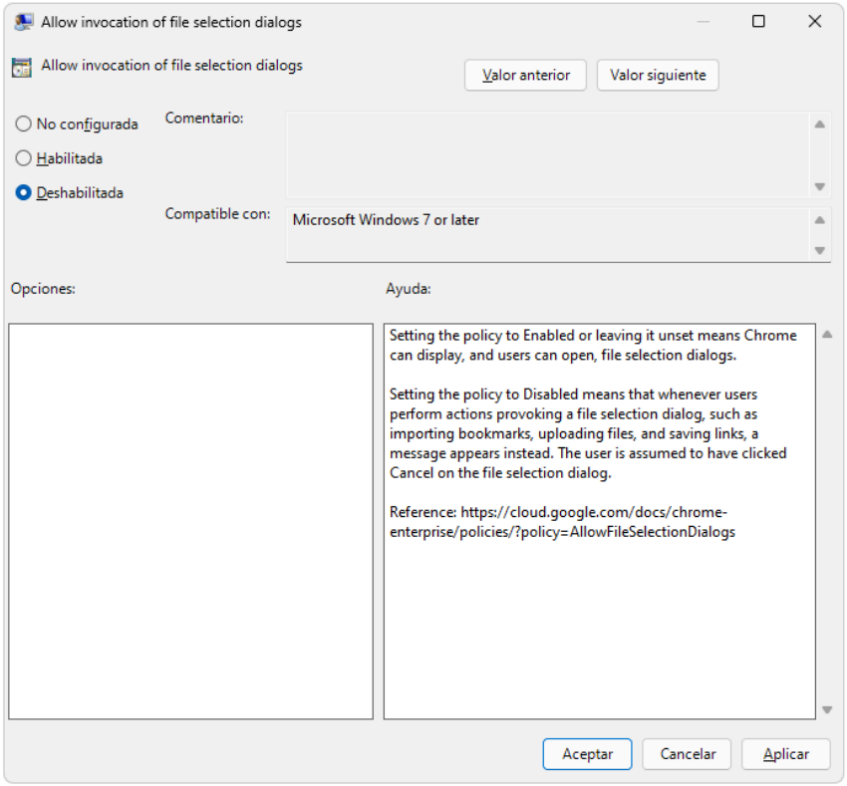
Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de

directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:AllowFileSelectionDialogs
```

Corrección: para establecer la configuración recomendada a través de GP, establezca la siguiente ruta de acceso de la interfaz de usuario en Deshabilitado:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\Allow invocation of file selection dialogs
```



4.4 (L2) Ensure 'Allow or deny audio capture' is set to 'Disabled' (Automated)

Descripción: esta configuración permite a los administradores establecer si se solicita al usuario final acceso a los dispositivos de captura de audio.

- Deshabilitado (0): desactiva las indicaciones y la captura de audio solo funcionará para las direcciones URL configuradas en la lista AudioCaptureAllowedUrls.

- Habilitado (1): con la excepción de las direcciones URL establecidas en la lista AudioCaptureAllowedUrls, se solicita a los usuarios acceso a la captura de audio.

NOTA: La configuración afecta a todas las entradas de audio (no solo al micrófono incorporado). El estado recomendado para esta configuración es: Deshabilitado

Justificación: el usuario final que tiene la capacidad de permitir o denegar la captura de audio para sitios web en Google Chrome podría abrir una organización a un sitio malintencionado que puede capturar información de propiedad a través del navegador. Al limitar o no permitir la captura de audio, se elimina la discreción del usuario final, dejando en manos de la organización qué sitios pueden usar esta capacidad.

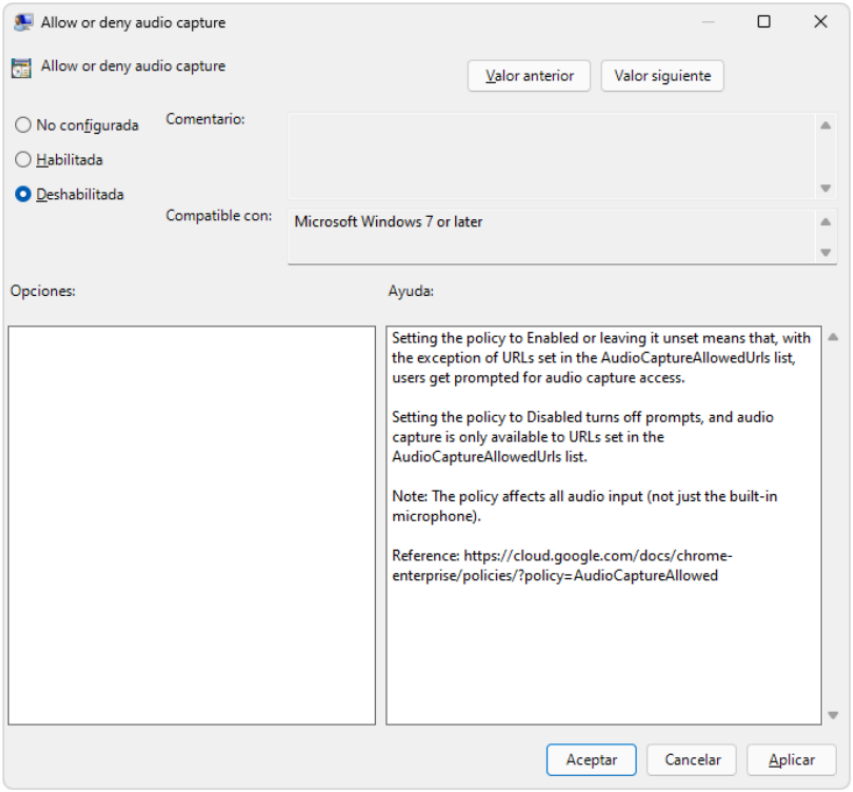
Impacto: Si deshabilita esta configuración, no se solicitarán dispositivos de audio a los usuarios cuando usen sitios web que puedan necesitar este acceso, como un sistema de conferencias basado en web. Si hay sitios a los que se permitirá el acceso, será necesaria la configuración de la configuración AudioCaptureAllowedUrls.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:AudioCaptureAllowed
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Deshabilitada:

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Allow or
deny audio capture
```



4.5 (L2) Ensure 'Allow or deny video capture' is set to 'Disabled' (Automated)

Descripción: esta configuración permite a los administradores establecer si se solicita al usuario final acceso a los dispositivos de captura de vídeo.

- Deshabilitado (0): desactiva las indicaciones y la captura de vídeo solo funcionará para las direcciones URL configuradas en la lista VideoCaptureAllowedUrls.
- Habilitado (1): con la excepción de las direcciones URL establecidas en la lista VideoCaptureAllowedUrls, se solicita a los usuarios acceso a la captura de vídeo.

NOTA: El ajuste afecta a todas las entradas de vídeo (no solo a la cámara integrada). El estado recomendado para esta configuración es: Deshabilitado (0)

Justificación: El usuario final que tiene la capacidad de permitir o denegar la captura de vídeo para sitios web en Google Chrome podría abrir una organización a un sitio malintencionado que puede capturar información de propiedad a través del navegador. Al limitar o no permitir la captura de vídeo, se elimina la discreción del usuario final, dejando en manos de la organización qué sitios pueden utilizar esta capacidad.

Impacto: Si deshabilita esta configuración, no se solicitarán dispositivos de vídeo a los usuarios cuando utilicen sitios web que puedan necesitar este acceso, como un sistema

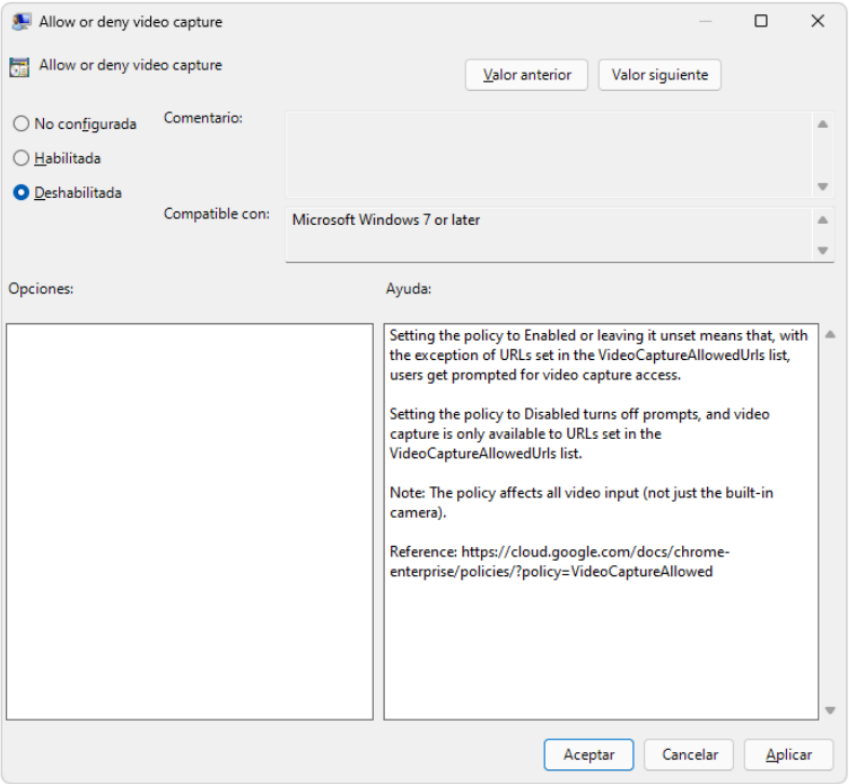
de conferencias basado en web. Si hay sitios a los que se permitirá el acceso, será necesaria la configuración de la configuración VideoCaptureAllowedUrls.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:VideoCaptureAllowed
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Deshabilitada:

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Allow or
deny video capture
```



4.6 (L1) Ensure 'Allow user feedback' is set to 'Disabled' (Automated)

Descripción: esta configuración controla si los usuarios pueden utilizar la función de comentarios de Chrome para enviar comentarios, sugerencias y encuestas a Google, así

como informes de problemas. El estado recomendado para esta configuración es: Deshabilitado (0)

Justificación: Los datos no deben compartirse con proveedores externos en un entorno administrado por la empresa.

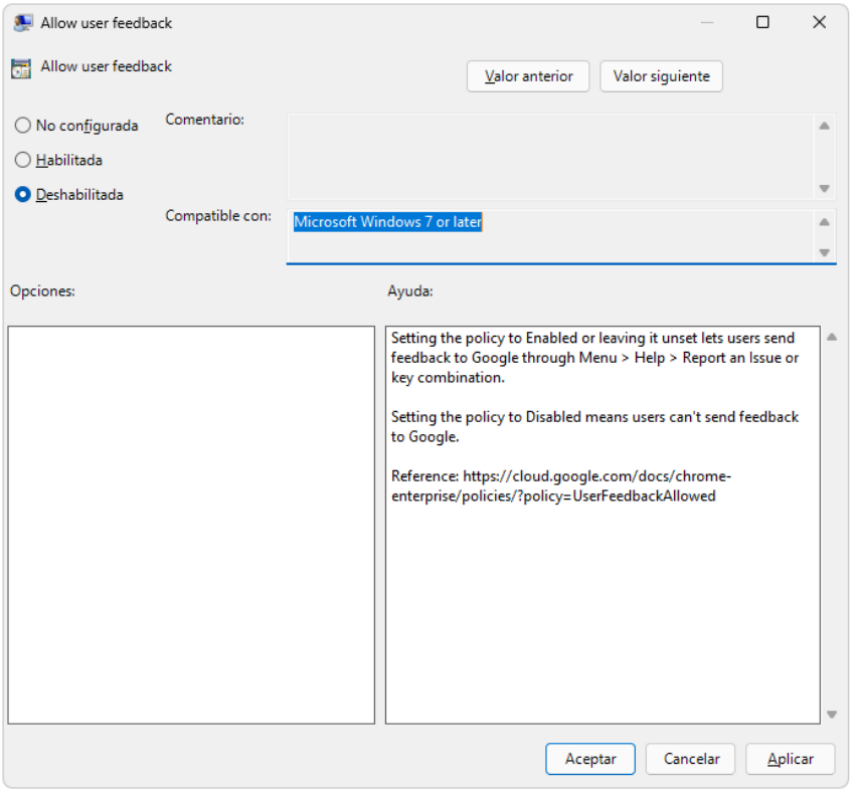
Impacto: Los usuarios no podrán enviar comentarios a Google.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:UserFeedbackAllowed
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Deshabilitada:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\Allow user feedback
```



4.7 (L2) Ensure 'Controls the mode of DNS-over-HTTPS' is set to 'Enabled: DNS-over-HTTPS without insecure fallback' (Automated)

Descripción: controla el modo de resolución de DNS a través de HTTPS. Tenga en cuenta que esta configuración solo establecerá el modo predeterminado para cada consulta. El modo se puede invalidar para tipos especiales de consultas, como solicitudes para resolver un nombre de host de servidor DNS a través de HTTPS.

- Deshabilitar DNS a través de HTTPS (desactivado)
- Habilitar DNS a través de HTTPS con reserva insegura (automático): habilite primero las consultas de DNS a través de HTTPS si hay un servidor de DNS a través de HTTPS disponible y puede recurrir al envío de consultas inseguras en caso de error.
- Habilitar DNS-over-HTTPS sin reserva insegura (secure): solo envíe consultas de DNSover-HTTPS y no se resolverá en caso de error.

El estado recomendado para esta configuración es: Habilitado con un valor de Habilitar DNS-overHTTPS sin reserva insegura (seguro)

Nota: Al habilitar esta directiva, se recomienda configurar también la directiva DnsOverHttpsTemplates para que se establezcan las plantillas de URI. Puede obtener más información en el sitio de directivas empresariales DnsOverHttpsTemplates.

Justificación: DNS sobre HTTPS (DOH) tiene un par de beneficios principales:

1. Cifrar el tráfico de resolución de nombres DNS ayuda a ocultar sus actividades en línea, ya que DoH oculta las solicitudes de resolución de nombres del ISP y de cualquier persona que escuche en redes intermediarias.

2. DoH también ayuda a prevenir la suplantación de DNS y los ataques de intermediario (MitM).

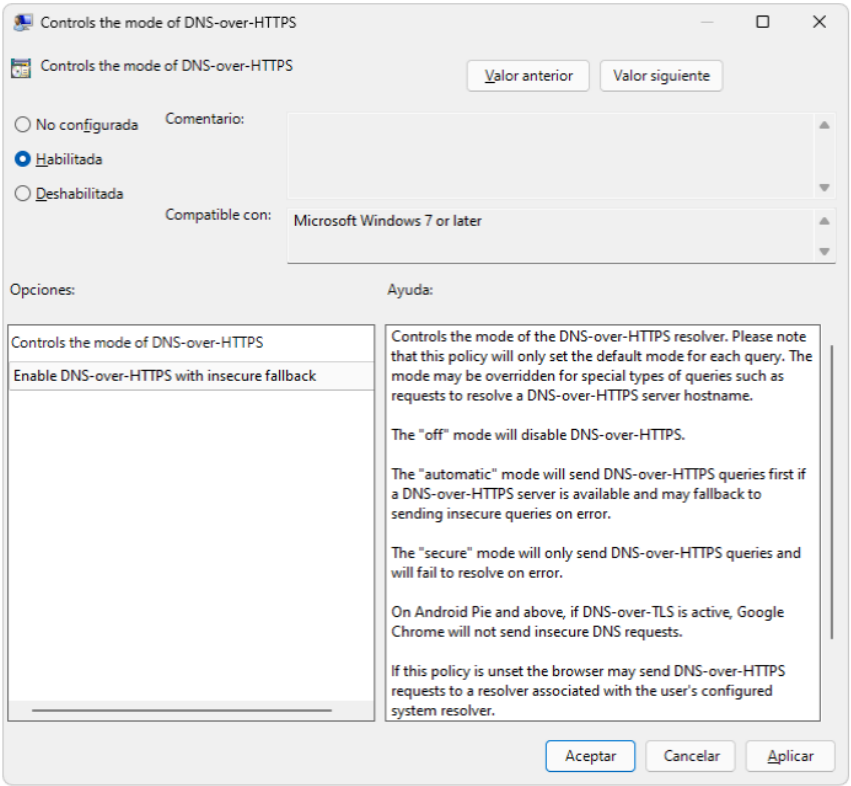
Impacto: No todos los proveedores de DNS son compatibles con DOH, por lo que las opciones son limitadas. Además, las empresas a veces supervisan las solicitudes de DNS para bloquear el acceso a sitios maliciosos o inapropiados. El monitoreo de DNS también se puede usar a veces para detectar malware que intenta "llamar a casa". Dado que DoH cifra las solicitudes de resolución de nombres, puede crear un punto ciego de supervisión de seguridad.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en secure:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:DnsOverHttpsMode
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Habilitada: Habilite DNS a través de HTTPS sin reserva insegura:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\Controls the mode of DNS-over-HTTPS
```



4.8 (L2) Ensure 'Enable AutoFill for addresses' is set to 'Disabled' (Automated)

Descripción: Chrome permite a los usuarios completar automáticamente formularios web con información guardada, como la dirección o el número de teléfono. Al deshabilitar esta función, se solicitará al usuario que ingrese toda la información manualmente. El estado recomendado para esta configuración es: Deshabilitado (0)

Justificación: Si un atacante obtiene acceso a la máquina de un usuario donde el usuario ha almacenado datos de autorrelleno de direcciones, se podría recopilar información. Impacto: Si esta configuración está deshabilitada, los usuarios no podrán acceder a Autocompletar.

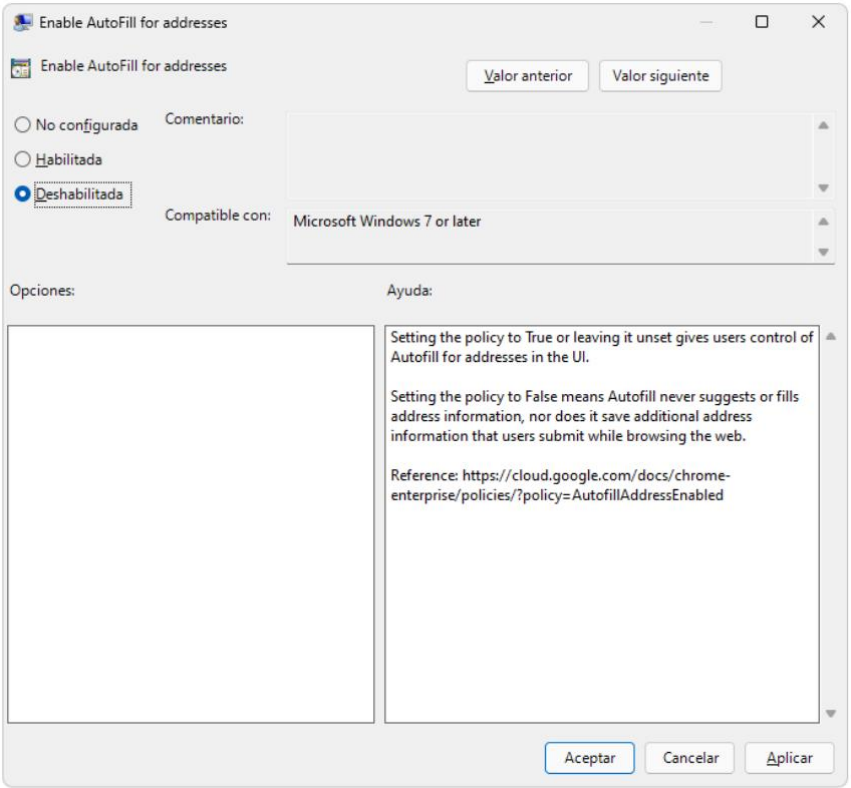
Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de

directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:AutofillAddressEnabled
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Deshabilitada:

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Enable
AutoFill for addresses
```



4.9 (L1) Ensure 'Enable AutoFill for credit cards' is set to 'Disabled' (Automated)

Descripción: Chrome permite a los usuarios completar automáticamente formularios web con la información de la tarjeta de crédito guardada. Al deshabilitar esta función, se solicitará al usuario que ingrese toda la información manualmente. El estado recomendado para esta configuración es: Deshabilitado (0)

Justificación: si un atacante obtiene acceso al equipo de un usuario donde el usuario ha almacenado datos de Autocompletar de tarjetas de crédito, se podría recopilar información.

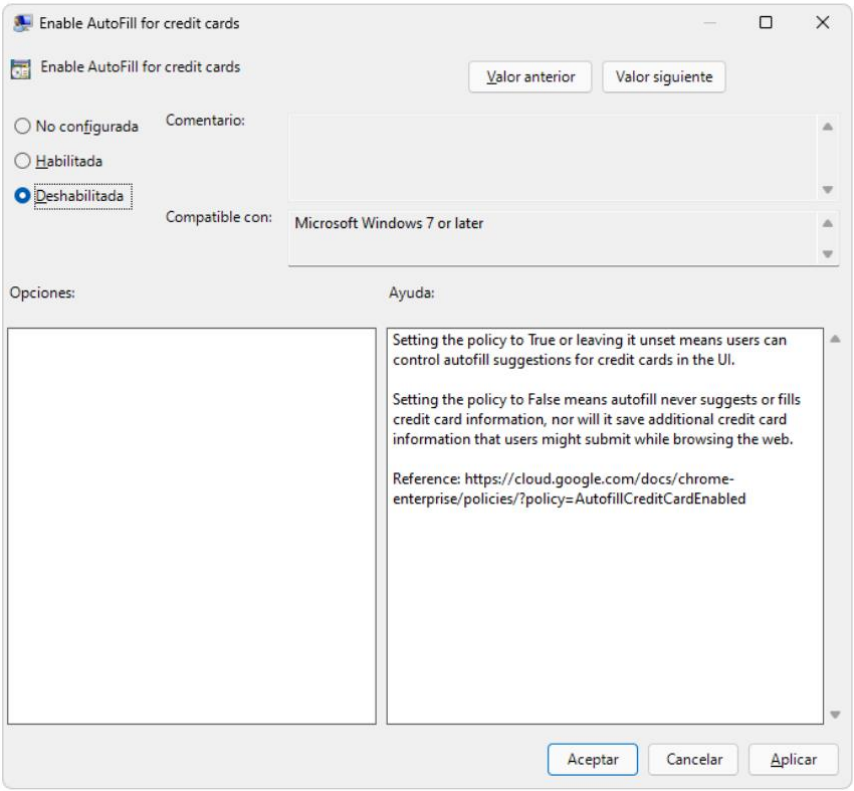
Impacto: Si esta configuración está deshabilitada, los usuarios no podrán acceder a la función Autocompletar de la tarjeta de crédito.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:AutofillCreditCardEnabled
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Deshabilitada:

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Enable
AutoFill for credit cards
```



4.10 (L1) Ensure 'Import saved passwords from default browser on first run' is set to 'Disabled' (Automated)

Descripción: esta configuración controla si las contraseñas guardadas desde el navegador predeterminado se pueden importar (en la primera ejecución y luego manualmente). El estado recomendado para esta configuración es: Deshabilitado (0)

Justificación: En Chrome, las contraseñas se pueden almacenar en texto sin formato y se pueden revelar haciendo clic en el botón "mostrar" junto al campo de contraseña yendo a chrome://settings/passwords/.

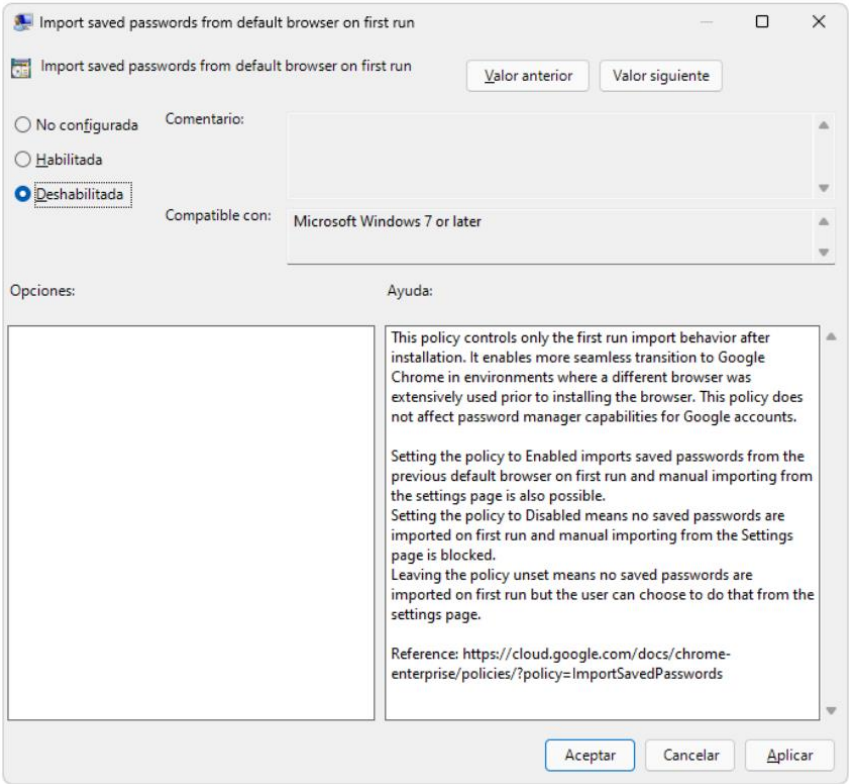
Impacto: Si esta configuración está deshabilitada, las contraseñas guardadas de otros navegadores no se importan.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:ImportSavedPasswords
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Deshabilitada:

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Import
saved passwords from default browser on first run
```



4.11 (L1) Ensure 'List of types that should be excluded from synchronization' is set to 'Enabled: passwords' (Automated)

Descripción: esta configuración le permite especificar los tipos de datos que se limitarán o excluirán de la carga de datos en el servicio de sincronización de Google Chrome. El estado recomendado para esta configuración es: Habilitado con las siguientes contraseñas de valor de texto (distingue entre mayúsculas y minúsculas)

NOTA: Se pueden incluir otras configuraciones además de las contraseñas en función de las necesidades de la organización.

Justificación: Almacenar y compartir información podría exponer información confidencial, incluidas, entre otras, las contraseñas de los usuarios y la información de inicio de sesión. Permitir esta sincronización también podría permitir que un usuario final extrajera datos corporativos que se sincronizaron en la nube a una máquina personal.

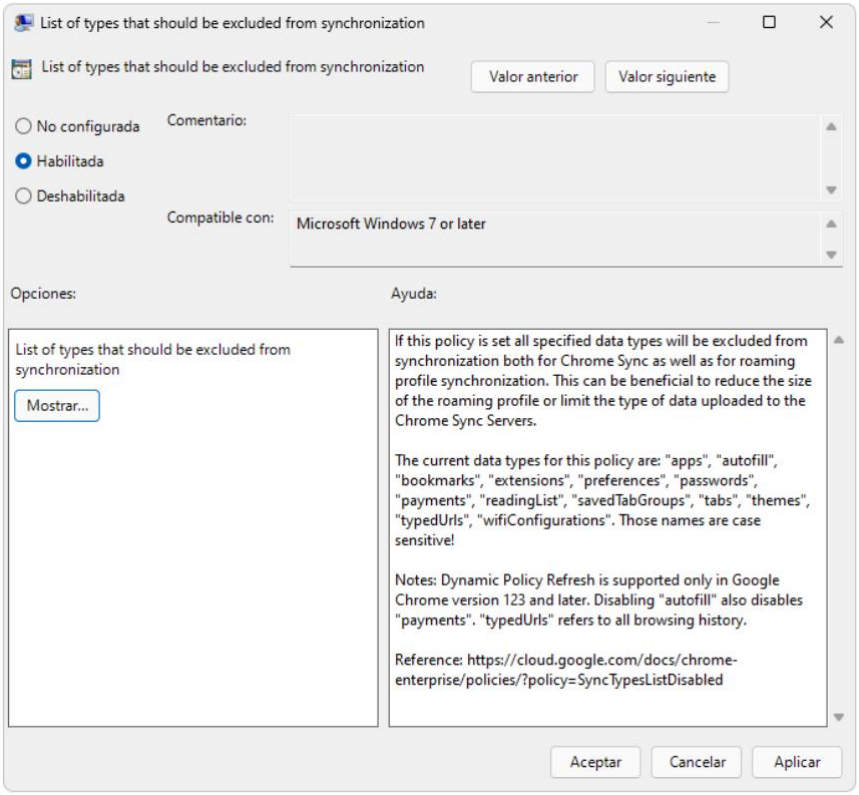
Impacto: Los datos de las contraseñas no se sincronizarán con el servicio de sincronización de Google Chrome.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en contraseñas:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\SyncTypesListDisabled:1
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Habilitado: contraseñas (distingue entre mayúsculas y minúsculas):

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\List of types that should be excluded from synchronization
```



4.12 (L2) Ensure 'Allow or deny screen capture' is set to 'Disabled' (Automated)

Descripción: si está habilitada o no configurada (valor predeterminado), una página web puede usar API de pantalla compartida (por ejemplo, getDisplayMedia() o la API de extensión de Desktop Capture) para solicitar al usuario que seleccione una pestaña, una ventana o un escritorio para capturar.

Justificación: El usuario final que tiene la capacidad de permitir o denegar la captura de pantalla de los sitios web en Google Chrome podría exponer a una organización a un sitio malicioso que puede capturar información confidencial a través del navegador. Al limitar o no permitir la captura de pantalla, se elimina la discreción del usuario final, dejando en manos de la organización qué sitios pueden usar esta capacidad.

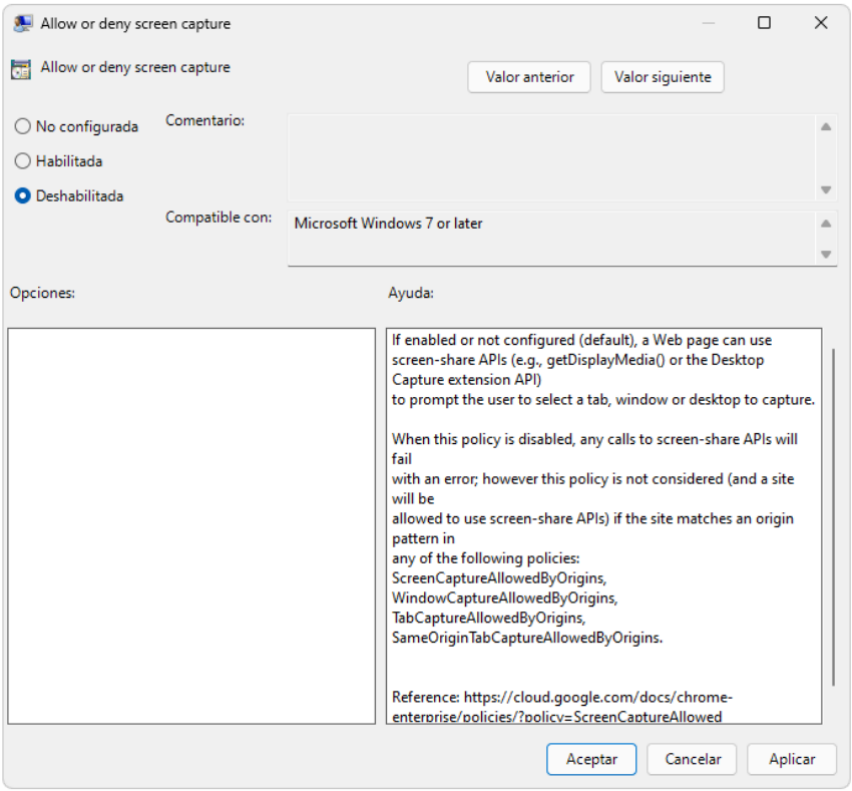
Impacto: Cuando esta directiva está deshabilitada, se producirá un error en las llamadas a las API de uso compartido de pantalla. Esta directiva no se tiene en cuenta (y un sitio podrá usar las API de uso compartido de pantalla) si el sitio coincide con un patrón de origen en cualquiera de las siguientes directivas: ScreenCaptureAllowedByOrigins, WindowCaptureAllowedByOrigins, TabCaptureByOrigins, SameOriginTabCaptureAllowedByOrigins.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:ScreenCaptureAllowed
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Deshabilitada:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\Allow or deny screen capture\Allow or deny screen capture
```



5 Forensics (Post Incident)

Esta sección contiene recomendaciones para ayudar en el análisis forense posterior al incidente. Las organizaciones deben revisar esta configuración y los posibles impactos para asegurarse de que tengan sentido dentro de su entorno

5.1 (L2) Ensure 'Enable guest mode in browser' is set to 'Disabled' (Automated)

Descripción: esta configuración controla si un usuario puede utilizar perfiles de invitado en Google Chrome. El estado recomendado para esta configuración es: Deshabilitado (0)

Justificación: En un perfil de invitado, el explorador no importa los datos de navegación de los perfiles existentes y elimina los datos de navegación cuando se cierran todos los perfiles de invitado. Al eliminar los datos del navegador, se eliminará la información que puede ser importante para una investigación informática, y es posible que los investigadores, como los analistas forenses informáticos, no puedan recuperar la información pertinente para la investigación.

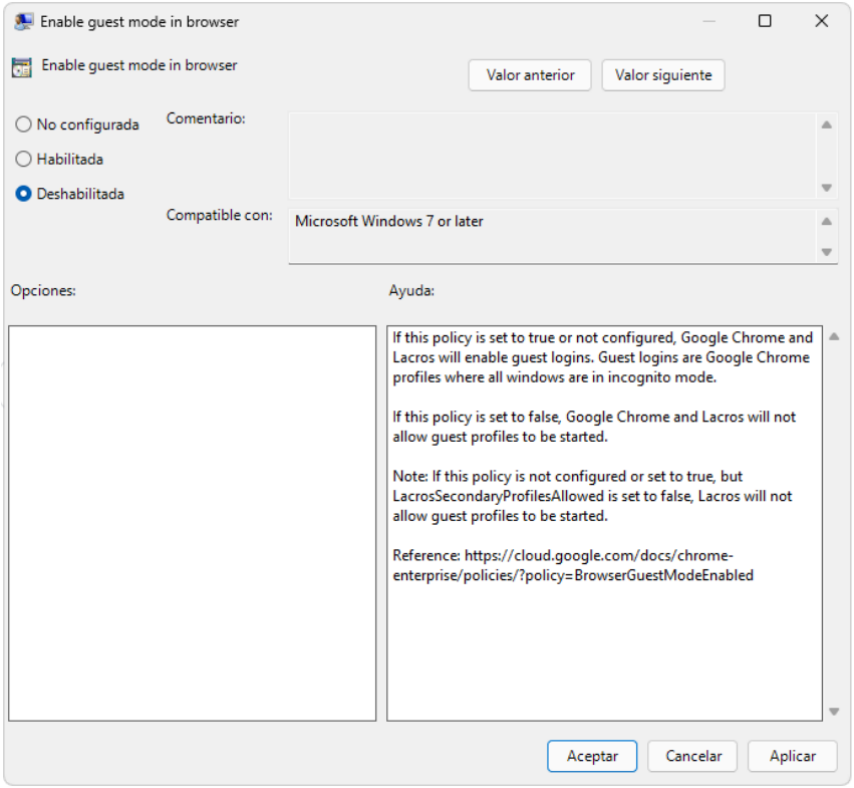
Impacto: Los usuarios no podrán iniciar el modo de invitado en Google Chrome.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:BrowserGuestModeEnabled
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Deshabilitada:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\Enable guest mode in browser
```



5.2 (L2) Ensure 'Incognito mode availability' is set to 'Enabled: Incognito mode disabled' (Automated)

Descripción: especifica si el usuario puede abrir páginas en modo incógnito en Google Chrome. Los valores posibles son:

- Modo incógnito disponible (0 - Igual que Desactivado))
- Modo incógnito desactivado (1)
- Modo incógnito forzado (2) El estado recomendado para esta configuración es: Habilitado: Modo incógnito desactivado (1)

Justificación: El modo incógnito de Chrome te ofrece la opción de navegar por Internet sin que tu actividad se guarde en tu navegador o dispositivo. Permitir que los usuarios usen el navegador sin que se guarde ninguna información puede ocultar evidencia de comportamientos maliciosos. Esta información puede ser importante para una investigación informática, y es posible que los investigadores, como los analistas forenses informáticos, no puedan recuperar la información pertinente para la investigación.

Impacto: Los usuarios no podrán iniciar el modo incógnito en Google Chrome.

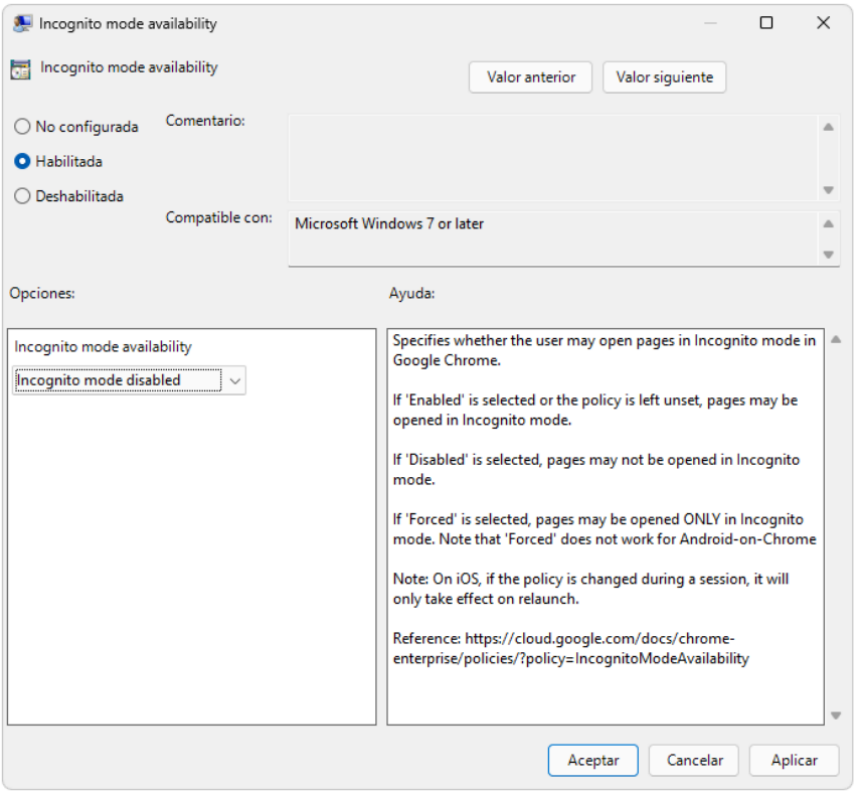
Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de

directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en 1:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:IncognitoModeAvailability
```

Corrección: Para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Habilitado: Modo incógnito deshabilitado:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\Incognito mode availability
```



5.3 (L1) Ensure 'Set disk cache size, in bytes' is set to 'Enabled: 250609664' (Automated)

Descripción: esta configuración controla el tamaño de la memoria caché, en bytes, que se utiliza para almacenar archivos en el disco. El estado recomendado para esta configuración es: Habilitado: 250609664 o superior

NOTA El valor especificado en esta configuración no es un límite estricto, sino una sugerencia para el sistema de almacenamiento en caché; Cualquier valor por debajo de unos pocos megabytes es demasiado pequeño y se redondeará a un mínimo razonable.

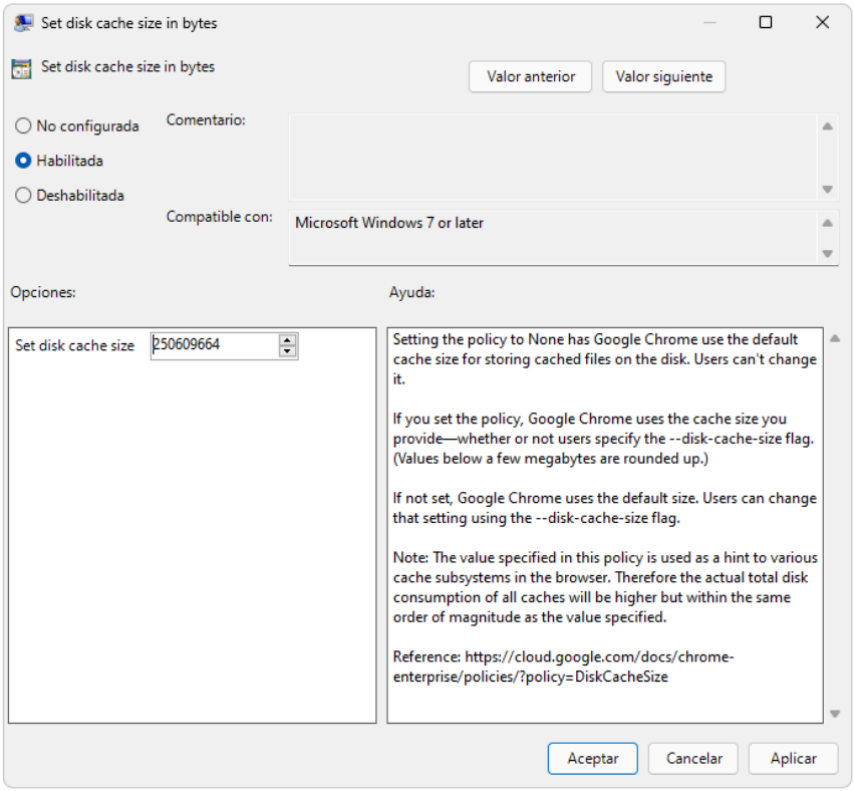
Justificación: Tener suficiente espacio en disco para la caché del navegador es importante para una investigación informática y para que los investigadores, como los analistas forenses informáticos, puedan recuperar la información pertinente para la investigación. Impacto: La caché del navegador ocupará hasta 250 MB de espacio en disco.

Auditoría: Vaya a la ruta de acceso de la interfaz de usuario articulada en la sección Corrección y confirme que está configurada según lo prescrito. Esta configuración de directiva de grupo está respaldada por la siguiente ubicación del Registro, que debe establecerse en ef00000 (250609664 en formato hexadecimal):

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:DiskCacheSize
```

Corrección: para establecer la configuración recomendada a través de la directiva de grupo, establezca la siguiente ruta de acceso de la interfaz de usuario en Habilitada: 250609664:

```
Computer Configuration\Policies\Administrative Templates\Google\Google
Chrome\Set disk cache size in bytes
```



Conclusión

En conclusión, la implementación de las recomendaciones del manual **CIS para Chrome** es un paso fundamental para aumentar la seguridad de nuestro navegador, ya sea en el entorno doméstico o laboral. Este proyecto ha demostrado cómo la modificación de las configuraciones de Chrome, siguiendo las directrices de este manual, puede contribuir significativamente a minimizar los riesgos asociados con el uso del navegador.

Sin embargo, es crucial recordar que la seguridad en línea es un proceso continuo y no un destino final. Es imprescindible mantenerse actualizado con las últimas versiones del manual y adaptar las configuraciones en consecuencia. De esta manera, podemos garantizar que Chrome no solo sea fácil de usar, sino también un espacio seguro para navegar por internet. Mantenerse seguro en línea es una tarea que nunca termina, pero con las herramientas y conocimientos adecuados, podemos hacer de la web un lugar más seguro para todos.