Manual de configuración segura

Gmail para empresas

Desde el **Centro de Protección Digital SURA** queremos acompañarte para que tu experiencia en el entorno digital sea confiable y tranquila. Para ello es necesario que con cada paso que des, tu información se encuentre siempre protegida. Por eso, te invitamos a leer y poner en práctica las siguientes recomendaciones para la configuración segura de cuentas de correo en Gmail.

Nota: *las instrucciones que encontrarás a continuación están diseñadas para realizarlas en los sitios web de las aplicaciones, es decir, desde un computador. Esto se debe a que la configuración de seguridad de las aplicaciones desde la versión móvil varía según el tipo de celular. Al realizar la configuración desde la web, esta quedará aplicada en tu cuenta para tus dispositivos personales. De igual manera Las imágenes mostradas a continuación, fueron utilizadas como ejemplo para ilustrar el proceso, ciertas opciones pueden variar de acuerdo a tu configuración regional e idioma*

Para Iniciar el proceso de configuración de seguridad y privacidad, ingresa a la cuenta administradora de Gmail.

1. Haz clic en el icono superior derecho y luego en ***Administra tu Cuenta de Google***.

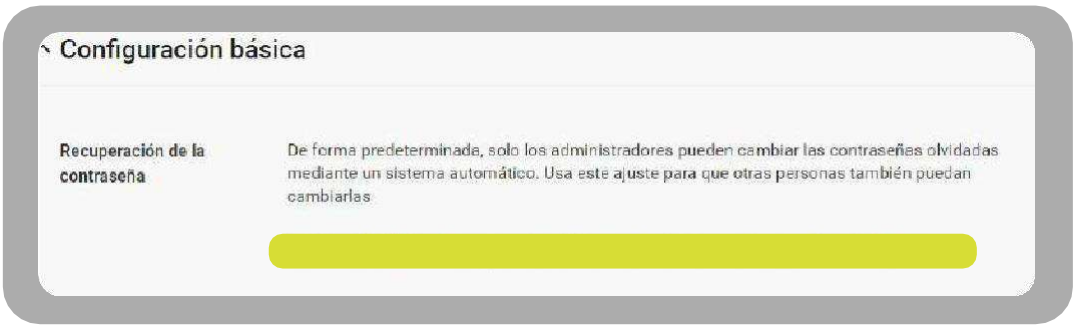
2. Posteriormente, busca este icono:

3 Observarás una imagen como la siguiente. Ahora puedes hacer clic en ***Configuración básica***.

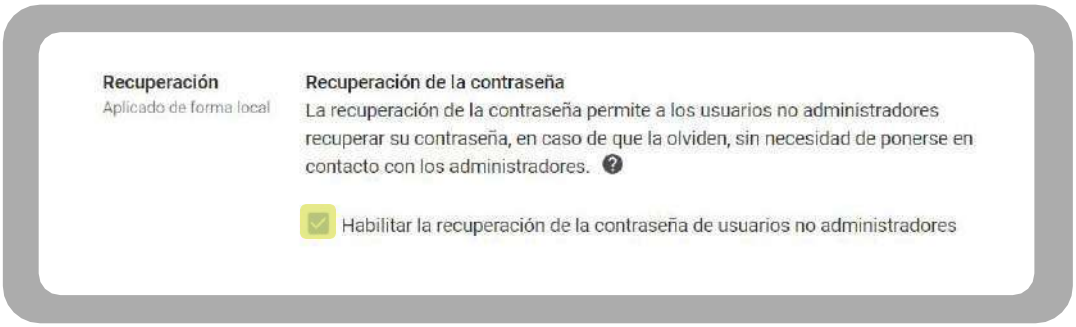
4 A continuación, se desplegarán varias opciones.

5 **Recuperación de la contraseña.**

Haz clic en ***Habilitar/inhabilitar la recuperación de la contraseña de usuarios no administradores***. Esta opción permite que los usuarios o empleados de tu organización puedan realizar autogestión de la recuperación de la contraseña.



Selecciona la opción ***Habilitar la recuperación de la contraseña de usuarios no administradores***.

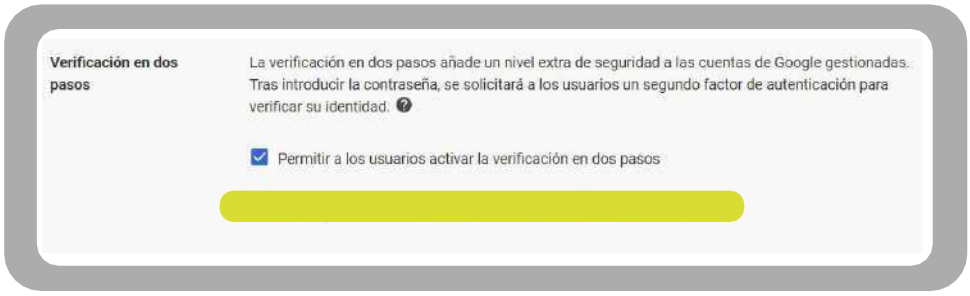


Regresa al menú principal de Seguridad y selecciona la opción ***Validación en dos pasos***.

6 Verificación en dos pasos

La verificación en dos pasos o segundo factor de autenticación disminuye el riesgo a que personas inescrupulosas o no autorizadas ingresen a tu plataforma de correo.
Para activarla, selecciona la opción ***Permitir a los usuarios activar la verificación en dos pasos***.

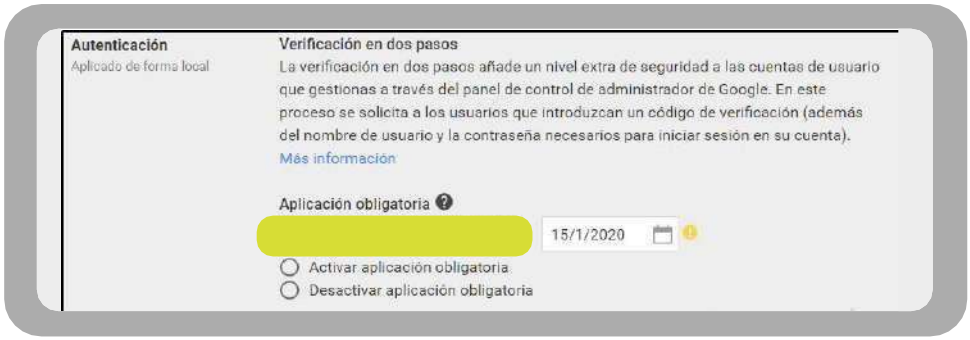
Posteriormente, haz clic en ***Ir a la configuración avanzada para requerir la verificación en dos pasos***, como ves en la siguiente imagen:



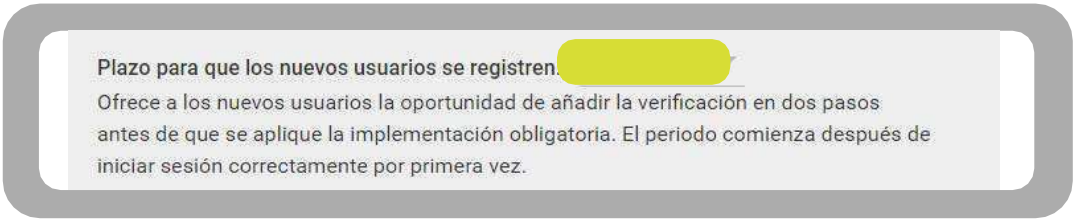
En la configuración avanzada para la verificación en dos pasos se desplegarán las siguientes opciones:

- Aplicación obligatoria
- Plazo para que los nuevos usuarios se registren
- Método de verificación en dos pasos

Para la ***Aplicación obligatoria*** es recomendable que sea obligatoria para todas las personas de la organización. Adicionalmente, te sugerimos poner un plazo para divulgar esta nueva política de seguridad entre tus empleados.

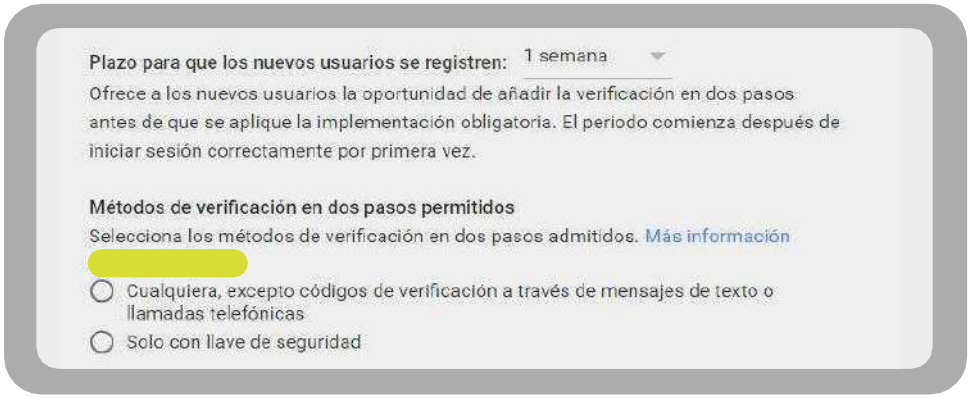


Para el Plazo para que los nuevos usuarios se registren, posterior a la divulgación de la obligatoriedad se recomienda dar entre 1y 2 semanas, para que los usuarios se vayan registrando en este tiempo. Posterior a su finalización el sistema lo define obligatorio para el que haya faltado habilitar el método de autenticación en dos pasos.



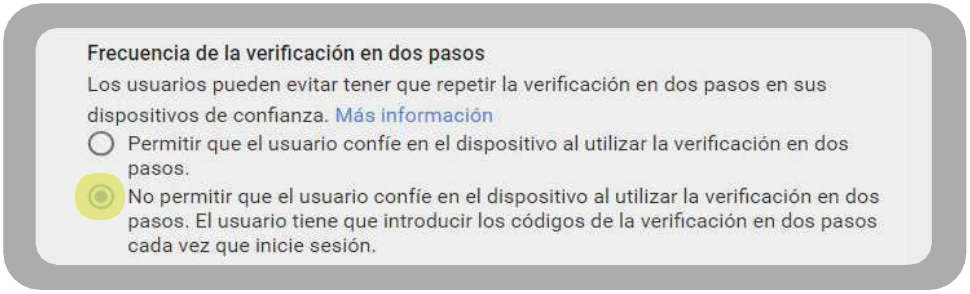
Para el ***Método de verificación en dos pasos permitidos***, selecciona la opción ***Cualquiera***. Esta permite utilizar cualquiera de los métodos disponibles: mensaje de texto al celular (SMS/MMS) o llamada telefónica, aplicativos de verificación en dos pasos y llaves de seguridad.

Nota: te recomendamos que el método de verificación en dos pasos se realice por medio de apps, esto debido a que por SMS/MMS estarías expuesto al ataque cibernético conocido como SIM swapping (duplicación de SIM).



En la opción ***Frecuencia de la verificación en dos pasos***, selecciona: *No permitir que el usuario confíe en el dispositivo al utilizar la verificación en dos pasos. El usuario tiene que introducir los códigos de la verificación en dos pasos cada vez que inicie sesión.*

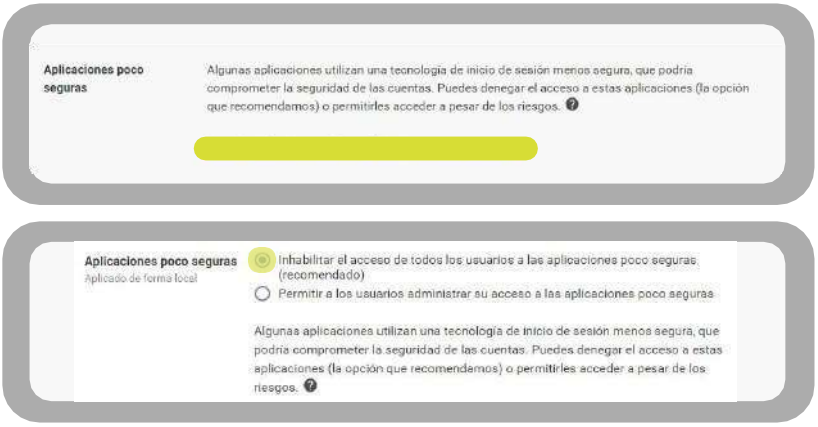
De esta manera, cada vez que se inicie sesión en el correo, se pedirá el segundo factor de autenticación.



Posterior a realizar la configuración avanzada del segundo factor de autenticación, regresa al menú principal de Seguridad y selecciona la opción ***Aplicaciones poco seguras***.

7 Aplicaciones poco seguras

Esta opción se activa para evitar que otras aplicaciones ajenas a la herramienta Google sean usadas para iniciar la sesión en el correo electrónico.
Haz clic en ***Acceder a los ajustes de las aplicaciones poco seguras***.

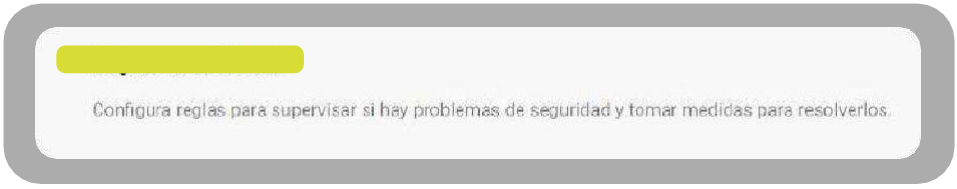


Selecciona la opción: ***Inhabilitar el acceso de todos los usuarios a las aplicaciones poco seguras***. De esta manera incrementas los niveles de seguridad de la plataforma del correo electrónico, al no permitir el uso de otras aplicaciones menos seguras.

Posterior a inhabilitar las aplicaciones poco seguras, regresa al menú principal de Seguridad para chequear las ***Reglas de actividad***.

8 Reglas de actividad

Esta opción se activa para evitar que otras aplicaciones ajenas a la herramienta Google sean usadas para iniciar la sesión en el correo electrónico.
Haz clic en ***Acceder a los ajustes de las aplicaciones poco seguras***.



Las reglas de actividad permiten gestionar gran parte de la seguridad de tu plataforma de correo electrónico. Existen más de 50 reglas de actividad pero, para ejemplificar, te mostraremos algunas de las que se pueden configurar en la plataforma:

- Contraseña filtrada
- Se cambió la configuración de correo electrónico
- Se activa a un usuario suspendido
- Acceso sospechoso
- Se otorgó privilegio de administrador al usuario
- Se cambió la contraseña de un usuario
- Un remitente envió mensajes a tu dominio que los usuarios clasificaron como suplantación de identidad (phishing)

Nota: Es importante validar todas las reglas configuradas por defecto, con el fin de analizar la pertinencia y activar las que se consideren necesarias de acuerdo con la actividad de la plataforma del correo. Si tienes alguna inquietud, recuerda consultar con un experto en ciberseguridad.

Posterior a validar las reglas de actividad, regresa al menú principal de Seguridad y haz clic en ***Gestión de contraseñas***.

9 Gestión de contraseñas

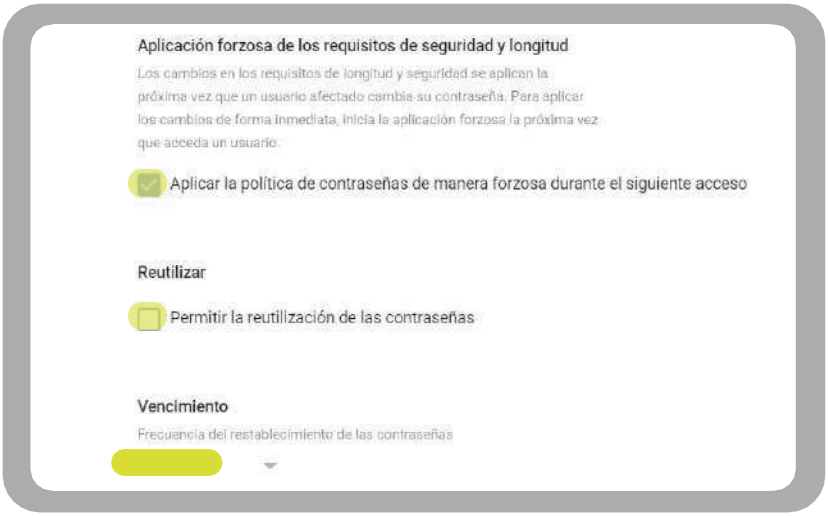
Otra parte importante de la seguridad en Gmail es establecer políticas para la gestión de contraseñas. Por eso selecciona la opción: Configurar políticas de contraseña.

En la parte de ***Administración de las contraseñas*** algunos campos para configurar. Selecciona ***Aplicar la contraseña segura de manera forzosa***, con el fin de exigir a todos los empleados de la organización que utilicen las buenas prácticas en el manejo y creación de contraseñas seguras.

- Longitud de la Contraseña: Mínimo 12 caracteres
- Vencimiento: cada 90 días cambio de contraseña
- Reutilizar contraseñas: inhabilita esta función, de manera que no se reutilicen contraseñas viejas.

En la siguiente imagen puedes observar cómo se presenta la información:

Regresa al menú principal de Seguridad y ahora haz clic en ***Procedimientos de verificación de identidad***.



10 Procedimiento de verificación de identidad

Este ítem de configuración permite robustecer los niveles de seguridad de las cuentas de correo electrónico. Si sospechas que una persona no autorizada está intentando acceder a la cuenta de un usuario, esta opción solicita a dicha persona que responda una pregunta de seguridad adicional o que verifique su identidad. Por ejemplo, mediante el doble factor de autenticación.

Una vez hagas clic en ***Procedimiento de verificación de la identidad***, busca y selecciona la opción: Los inicios de sesión con SSO están sujetos a métodos de verificación adicionales (si corresponde) y a la verificación en dos pasos (si está configurada).

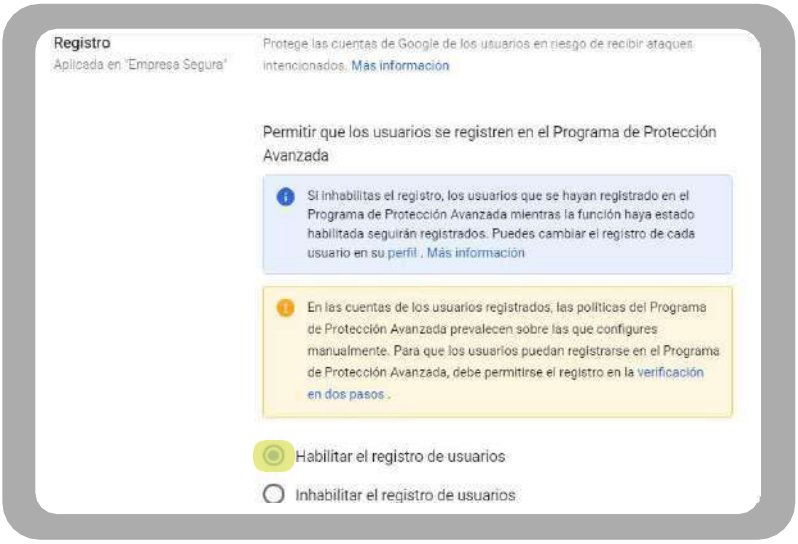
Ya puedes regresar al menú principal de Seguridad y buscar la opción ***Programa de Protección Avanzada***.

11 Programa de Protección Avanzada

Esta opción permite realizar configuraciones mucho más robustas y estrictas. Fue pensada para elevar los criterios de protección de las cuentas de correo electrónico de los empleados.

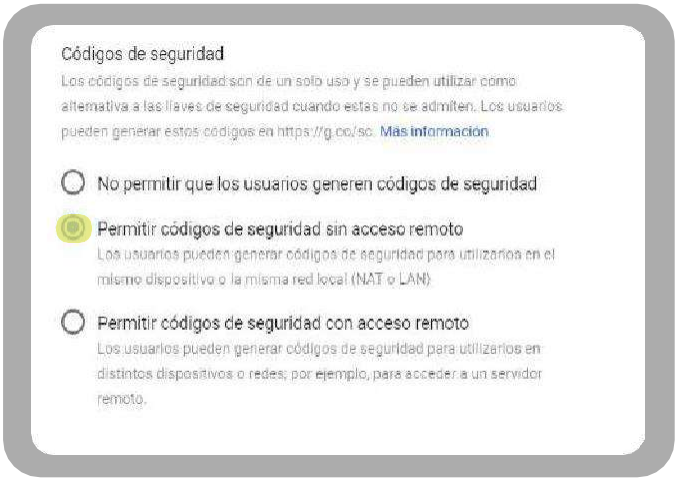
Registro

Te sugerimos registrar a todos los empleados de la empresa, seleccionando la opción ***Habilitar el Registro de Usuarios***.



Códigos de Seguridad

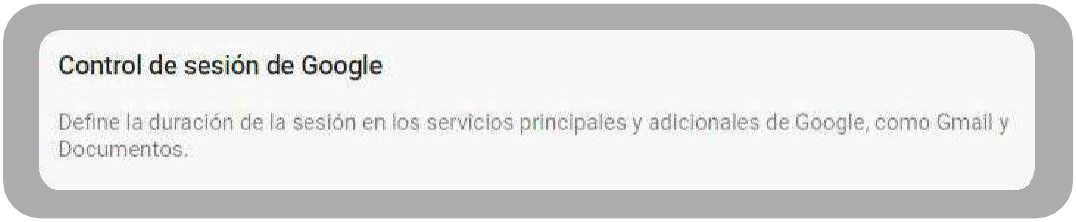
Los códigos de seguridad permiten el ingreso al correo electrónico y son una forma alternativa para entrar a la cuenta cuando perdemos la gestión de esta.
Nota: te recomendamos que, al habilitar esta opción, lo hagas con el acompañamiento de un experto en ciberseguridad, validando la pertinencia de la activación de estos códigos de acuerdo con las necesidades de tu empresa.

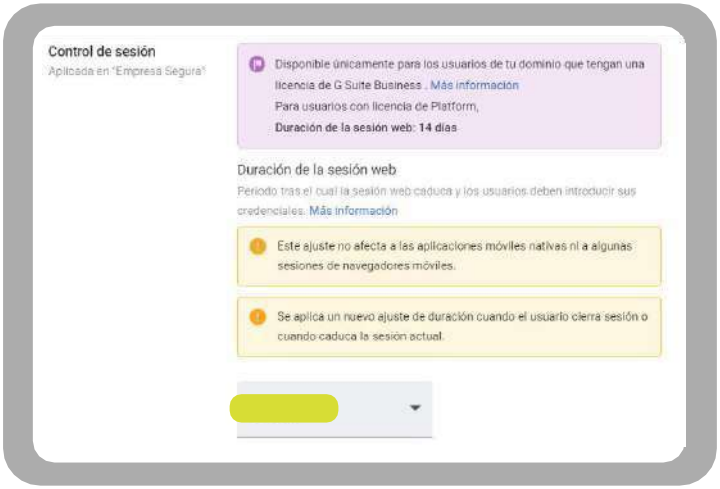


Regresa al menú principal de Seguridad y busca la opción **Control de sesión de Google.**

12 Control de sesión de Google

Esta función permite configurar cuánto tiempo puede permanecer activa una sesión de correo electrónico.



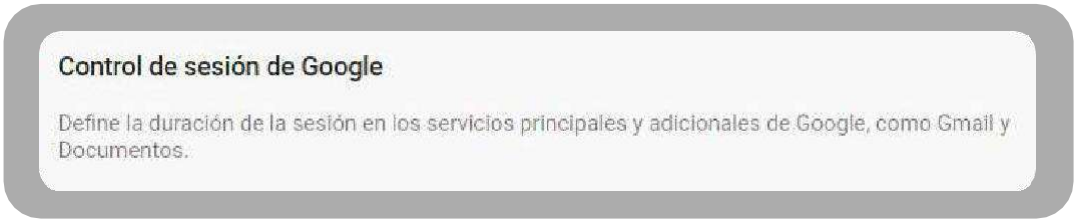


Es recomendable que a las 24 horas caduque la sesión, de manera que, al superar este tiempo, el sistema automáticamente la cierre. Cuando esto suceda, la plataforma pedirá al usuario volver a ingresar sus credenciales: nombre de usuario y contraseña.

Nota: si queremos definir esta política de manera más estricta, puedes reducir el tiempo de control de sesión a menos de 12 horas.

Ya puedes volver al menú principal de Seguridad para seleccionar la opción
Control de sesiones de Google Cloud (Beta)

13 Control de sesiones de Google Cloud (Beta)



Para el control de sesión de Google Cloud en su versión beta, también se recomienda que a las 24 horas caduque la sesión. Cuando esto suceda, la plataforma pedirá al usuario volver a ingresar sus credenciales: nombre de usuario y contraseña.

Nota: si queremos definir esta política de manera más estricta, puedes reducir el tiempo de control de sesión a menos de 12 horas.

Regresa al menú principal de Seguridad y ahora busca la opción ***Recursos de Seguridad y Privacidad***.

14 Recursos de Seguridad y Privacidad

Te recomendamos leer las políticas de seguridad y privacidad, con el fin de tener plena claridad sobre el compromiso de Google con la privacidad de los datos de sus usuarios.

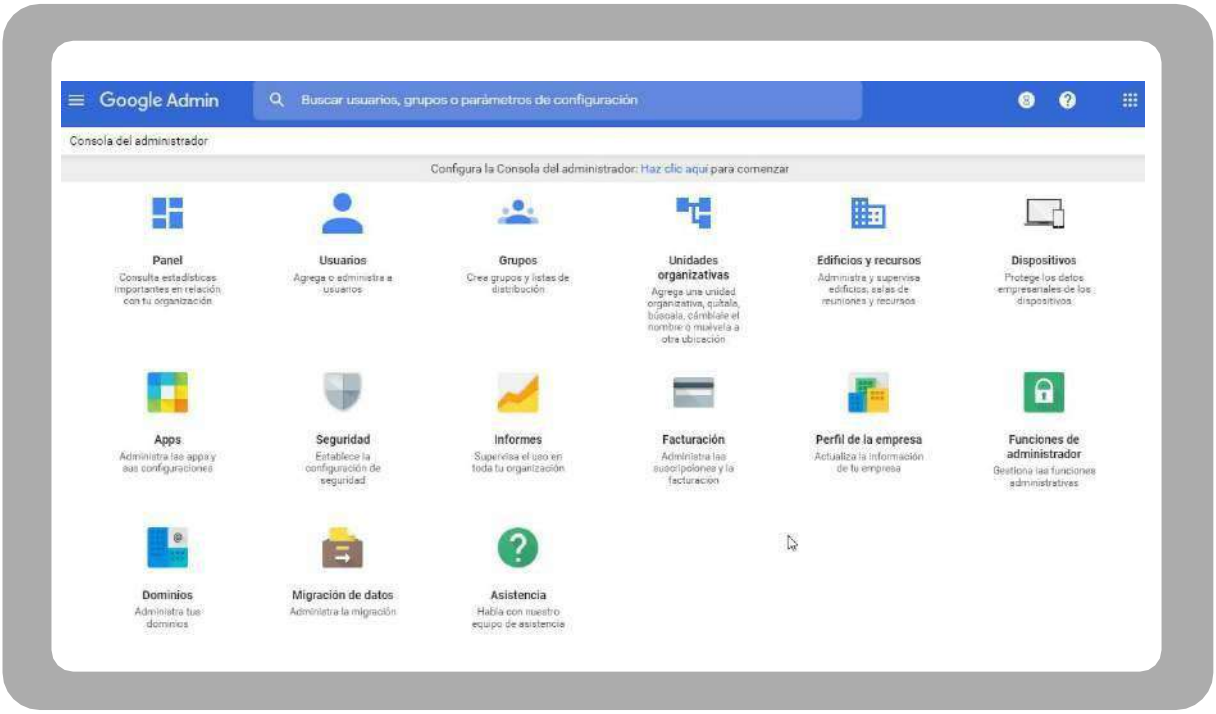
Ahora vuelve al menú principal de Seguridad y busca la opción ***Configuración avanzada***.

15 Configuración avanzada

Es importante que a la hora de realizar esta configuración, puedas estar acompañado por un equipo de expertos en administración de correo electrónico, o por un experto en ciberseguridad.

Para finalizar, recuerda que la consola de administración tiene otras funciones que vale la pena profundizar, con el fin de mantenerte informado sobre las buenas prácticas para la gestión de usuarios, grupos organizacionales, protección en dispositivos móviles, configuraciones de apps y funciones de administrador.

Procura verificarlas, ya que estas vienen configuradas por defecto. Y recuerda que en todo momento tienes la opción de comunicarte con el equipo de Google en la opción ***Asistencia***, donde podrás acudir a expertos en el área.



Configurar de forma adecuada tu cuenta de Gmail empresarial te permitirá gestionar la seguridad sobre tu entorno G-Suite en aplicaciones como YouTube, Pixel, Google Drive, Google My Business, Analytics, entre otras; así puedes estar protegido mientras haces uso de ellas.

Si deseas profundizar sobre las diferentes opciones, te invitamos a ingresar al sitio del fabricante Aquí

Centro de Protección Digital SURA

SURA, conectado con tu seguridad para que no te desconectes.

Conoce más aquí