

DOCUMENTACIÓN

Manual de la configuración en la consola de Administración previamente realizada

Autoría de: Karol Vanessa Nuñez Vera

Cargo: Aprendiz Sena

Dirigido a: Angela Patricia Marroquín y Jorge García

Fecha de realización: 04/04/2025

Tabla de contenido

1. Introducción

2. Acceso a la Consola del Administrador

- ¿Cómo iniciar sesión en la Consola del Administrador?
- Descripción general de la interfaz principal.

3. Configuración Global de la Verificación en Dos Pasos

- Navegación a la sección de Seguridad.
- Configuración de la política de Verificación en dos pasos para la organización:
- Permitir activación por usuarios.
- Implementación obligatoria.
- Plazo para nuevos usuarios.
- Frecuencia de la verificación.
- Métodos de verificación permitidos.
- Período de gracia.
- Códigos de seguridad.

3. Verificación del Estado en Usuarios Individuales

- Acceso al Directorio de Usuarios.
- Visualización de la información del usuario.

3.1 Revisión de la pestaña Seguridad del usuario:

- Estado de la Verificación en dos pasos.
- Información de recuperación.
- Métodos de verificación del usuario.

4. Conclusión

1. Introducción

¿Qué es la Verificación en Dos Pasos?

La verificación en dos pasos (también conocida como autenticación de dos factores o 2FA) es una capa adicional de seguridad para tu cuenta de Google Workspace. Requiere un segundo paso de verificación al iniciar sesión, además de tu contraseña, lo que dificulta el acceso no autorizado incluso si tu contraseña se ve comprometida. Este manual detalla el proceso de configuración de la verificación en dos pasos a nivel organizacional a través de la Consola del administrador de Google Workspace.

Objetivo de este Manual

Este manual tiene como objetivo guiar a los administradores de Google Workspace responsables de implementar y gestionar la seguridad de las cuentas de la organización a través de la configuración de la Verificación en dos Pasos. Adicionalmente, busca proporcionar una comprensión clara de los cambios realizados en esta configuración para cualquier persona interesada en profundizar en los aspectos de seguridad de Google Workspace.

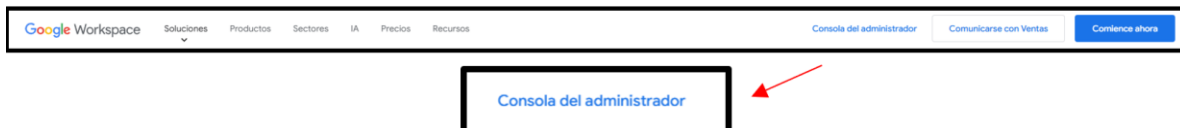
2. Acceso a la Consola del Administrador

Paso previo: Para llegar a la página principal de Google Workspace, puedes escribir Google Workspace o términos relacionados en la barra de direcciones de tu navegador y seleccionar el resultado oficial (generalmente el primero).

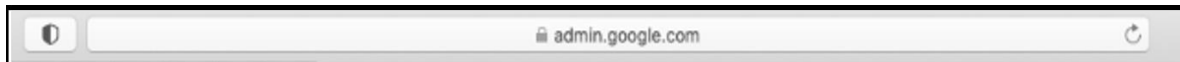
¿Cómo iniciar sesión en la Consola del Administrador?

Una vez en la página principal, si posees una cuenta con privilegios de administrador, tienes dos opciones principales para acceder a la Consola del administrador:

Opción 1: Buscar y seleccionar la opción que diga Consola del administrador. Esta generalmente se encuentra visible en la parte superior de la página.



Opción 2: Dirigirte directamente a la URL: admin.google.com en tu navegador.



Descripción general de la interfaz principal

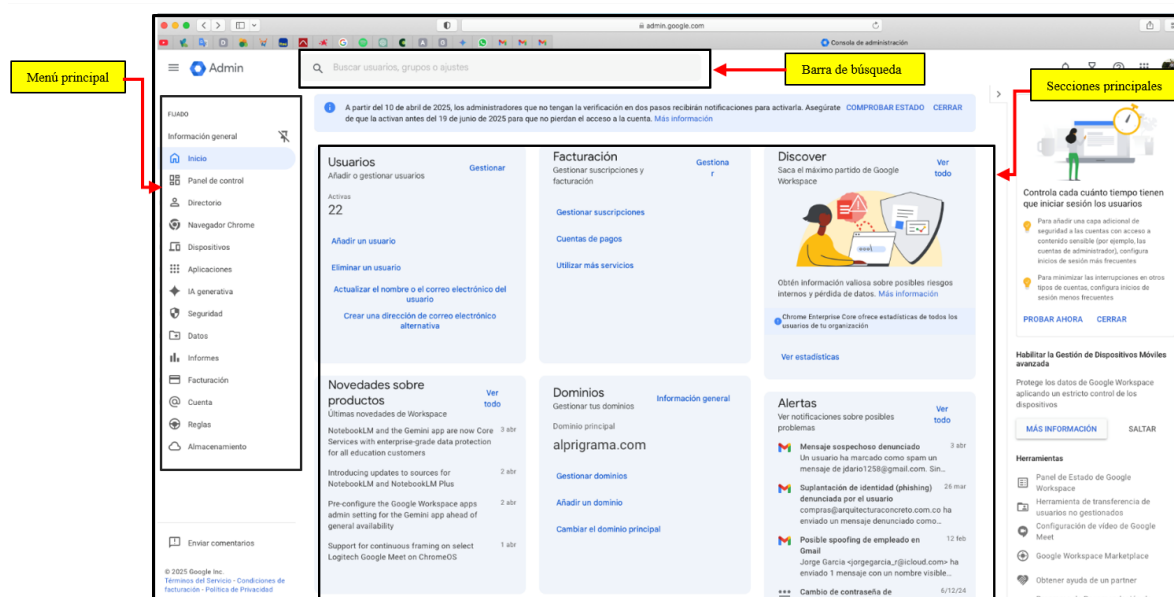
Al realizar esto, podrás identificar el menú principal, explorar el panel de control, reconocer la barra de búsqueda y observar las tarjetas o secciones principales de la página de inicio.

Los elementos principales que identificarás son:

- **Menú Principal (Lateral Izquierdo):** Esta barra vertical en el lado izquierdo de la pantalla es tu centro de navegación. Aquí encontrarás acceso a las diferentes secciones de administración, organizadas de forma lógica. Para la configuración de la Verificación en dos pasos, la sección clave es "Seguridad". Otras secciones importantes que explorarás son "Directorio" (para gestionar usuarios) y "Facturación" (para la gestión de suscripciones).

DOCUMENTACIÓN

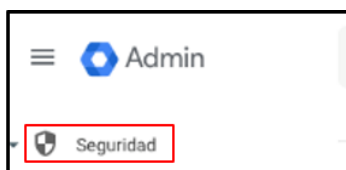
- **Barra de Búsqueda (Superior Central):** Ubicada en la parte superior, esta barra te permite buscar rápidamente usuarios, grupos, ajustes o funciones específicas dentro de la Consola. Si sabes el nombre de una sección o un ajuste, puedes usar la búsqueda para acceder directamente a él.
- **Panel de Información General (Página Central o secciones principales):** Al iniciar sesión, la página principal suele mostrar un resumen del estado de tu Google Workspace. Esta área presenta "tarjetas" o recuadros con información clave sobre usuarios, facturación, alertas y otras áreas importantes. Aunque útil para una visión general, para la configuración detallada de la Verificación en dos pasos, te dirigirás al menú principal.
- **Barra Superior (Derecha):** En la parte superior derecha, encontrarás iconos para acceder a funciones como notificaciones, ayuda, configuración de la cuenta de administrador y el selector de aplicaciones de Google.



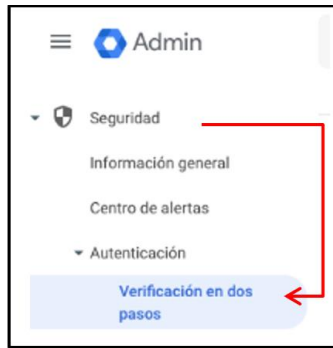
Navegación a la sección de Seguridad.

Para configurar la Verificación en dos pasos a nivel organizacional, he realizado los siguientes pasos:

Paso 1. Navegué hasta la sección de Seguridad dentro del menú principal de la Consola del administrador (barra lateral izquierda).



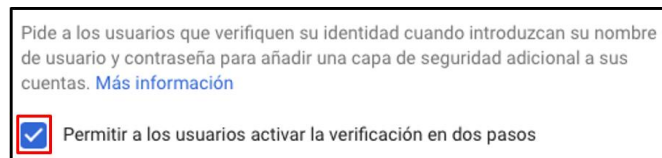
Paso 2. Dentro de **Seguridad**, seleccioné la opción "Verificación en dos pasos".



Configuración de la política de Verificación en dos pasos para la organización:

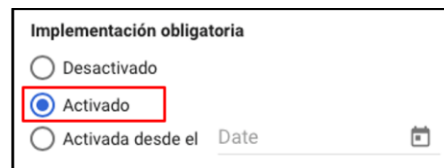
Permitir activación por usuarios.

Paso 3. En la sección **Autenticación**, marqué la casilla **Permitir a los usuarios activar la verificación en dos pasos**. Esto permite que los usuarios que lo deseen puedan habilitar esta capa de seguridad adicional en sus cuentas de forma individual.



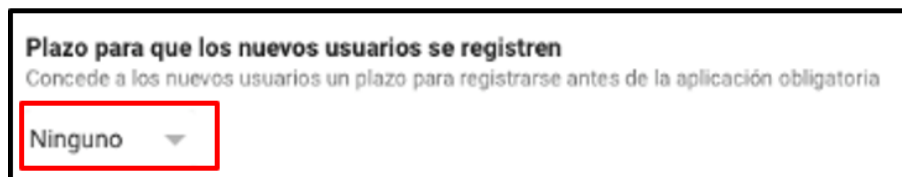
Implementación obligatoria.

Paso 4. En la sección **Implementación obligatoria**, he dejado la opción **Activado** seleccionada. Esto significa que actualmente la verificación en dos pasos es obligatoria para todos los usuarios de la organización.



Plazo para nuevos usuarios.

Paso 5. En **Plazo para que los nuevos usuarios se registren**, dejé la opción **Ninguno**. Esto implica que los nuevos usuarios no tienen un plazo específico para configurar la verificación en dos pasos. Podría haber establecido un periodo de gracia (ej. 7 días) si lo considerara necesario para dar tiempo a los nuevos usuarios a configurarlo.



Frecuencia de la verificación.

Paso 6. En la sección **Frecuencia**, seleccione **Permitir que el usuario confíe en el dispositivo**. Esto brinda a los usuarios la comodidad de no tener que ingresar un código de verificación en cada inicio de sesión desde dispositivos que marquen como confiables.

Frecuencia

Los usuarios no tendrán que repetir la verificación en dos pasos cuando inicien sesión en un dispositivo de confianza. [Más información](#)



Permitir que el usuario confíe en el dispositivo

Métodos de verificación permitidos.

Paso 7: En la sección **Métodos**, he asegurado que la opción **Cualquiera** esté seleccionada. Esto permite a los usuarios utilizar diversas formas de obtener códigos de verificación, como aplicaciones de autenticación, mensajes de texto o llamadas telefónicas.

Métodos

Selecciona el método que quieres aplicar de forma obligatoria. [Más información](#)



Cualquiera



Cualquiera, excepto códigos de verificación a través de mensajes de texto o llamadas telefónicas



Solo con llave de seguridad

Período de gracia.

Paso 8: En **Período de gracia de la suspensión de la política de verificación en dos pasos**, está configurado en **1 día**. Si un usuario tiene problemas con la verificación en dos pasos y se suspende temporalmente la política para su cuenta, tendrá un día para resolver el problema antes de que se vuelva a aplicar automáticamente.

Período de gracia de la suspensión de la política de verificación en dos pasos

Permite que los usuarios utilicen temporalmente códigos de verificación, además de sus llaves de seguridad, para iniciar sesión. El periodo de excepción de un usuario comienza cuando se generan los códigos de verificación.

1 día

Códigos de seguridad.

Paso 9: En cuanto a los **códigos de seguridad**, seleccioné la opción **Permitir códigos de seguridad sin acceso remoto**. Esta opción permite que los usuarios generen códigos de emergencia para iniciar sesión si tienen problemas con su celular u otro método de verificación. Pero estos códigos solo funcionarán en la misma computadora o red donde los crearon. Es una ayuda para momentos puntuales sin que alguien pueda usar esos códigos desde otro lugar. **(Insertar aquí una captura de pantalla de la sección "Códigos de seguridad" con la opción "Permitir códigos de seguridad sin acceso remoto" marcada).**

Códigos de seguridad

Los códigos de seguridad son de un solo uso y se pueden utilizar como alternativa a las llaves de seguridad cuando estas no se admiten. Los usuarios pueden generar estos códigos en <https://g.co/sc>. [Más información](#)



No permitir que los usuarios generen códigos de seguridad



Permitir códigos de seguridad sin acceso remoto

Los usuarios pueden generar códigos de seguridad para utilizarlos en el mismo dispositivo o la misma red local (NAT o LAN).



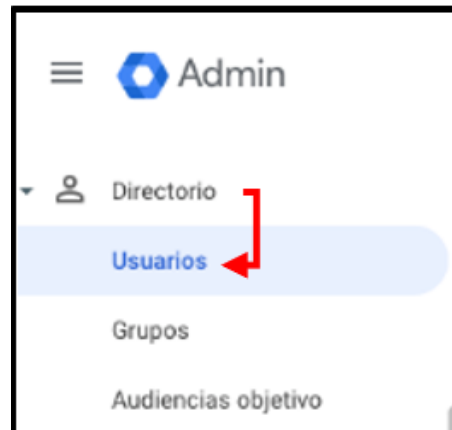
Permitir códigos de seguridad con acceso remoto

Los usuarios pueden generar códigos de seguridad para utilizarlos en distintos dispositivos o redes; por ejemplo, para acceder a un servidor remoto.

3. Verificación del Estado en Usuarios Individuales.

Paso 10: Una vez que he guardado la configuración de la Verificación en dos pasos a nivel organizacional, el siguiente paso lógico es observar cómo esta configuración se refleja en las cuentas de los usuarios. Para ello, navegué al **Directorio** desde el menú principal de la izquierda y luego seleccioné **Usuarios**.

Acceso al Directorio de Usuarios..



Esta sección mostrará la lista de todos los usuarios de la organización **alprigrama.com**. Desde aquí, como administrador, se pueden realizar diversas tareas de gestión de usuarios, como: Ver el estado de la Verificación en dos pasos, añadir nuevos usuarios, eliminar usuarios, modificar la información de los usuarios, restablecer contraseñas, suspender o reactivar usuarios, gestionar la pertenencia a grupos, entre otras funciones relacionadas con la administración de las cuentas de usuario.

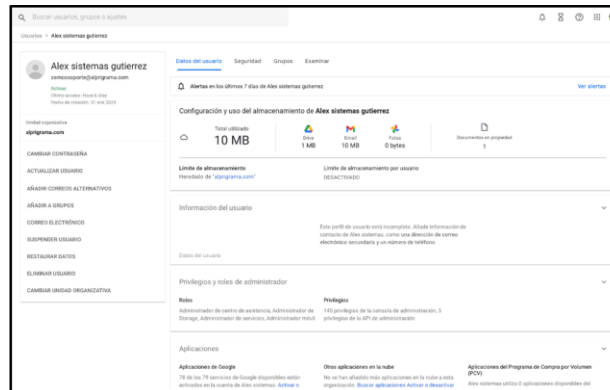


Paso 11: Al seleccionar un usuario específico de la lista en la sección **Directorio > Usuarios**, se abrirá una página con los detalles de esa cuenta. La primera pestaña que se muestra por defecto es la de **Datos del usuario**, como vemos en la siguiente captura de pantalla para el usuario Alex sistemas gutierrez.

Visualización de la información del usuario.

En esta sección, podemos observar diversa información importante sobre el usuario, incluyendo: Información básica (Nombre, correo electrónico principal, estado de la cuenta, fecha de la última actividad y fecha de creación), Unidad Organizativa, Acciones rápidas (menú en la izquierda), Uso de almacenamiento, Información del usuario (si el perfil está completo o no), Privilegios y roles de administrador, y Aplicaciones.

DOCUMENTACIÓN

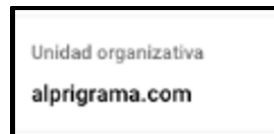


En esta sección, podemos observar diversa información importante sobre el usuario, incluyendo:

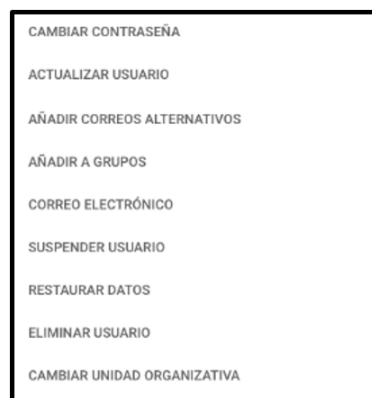
Información básica: Nombre, correo electrónico principal, estado de la cuenta (Activas), fecha de la última actividad y fecha de creación.



Unidad Organizativa: A la que pertenece el usuario dentro de la estructura de la organización.

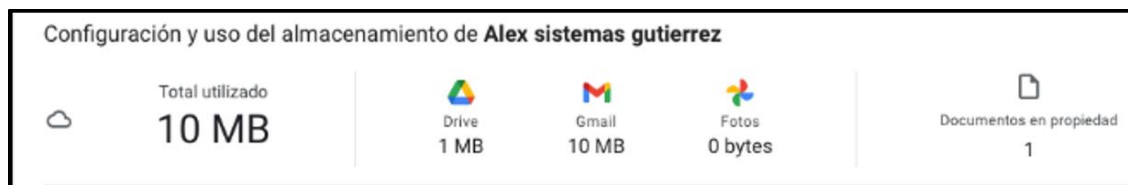


Acciones rápidas: Un menú en la parte izquierda que permite realizar acciones comunes para este usuario, como cambiar su contraseña, actualizar su información, añadir correos alternativos, gestionarlo en grupos, etc.



Uso de almacenamiento: Un resumen del espacio de almacenamiento total utilizado por el usuario y la distribución entre los diferentes servicios de Google Workspace (Drive, Gmail, Fotos). También se indica si tiene un límite de almacenamiento específico o si hereda la política de la organización.

DOCUMENTACIÓN



Información del usuario: (En este caso, se indica que el perfil está incompleto, lo cual también es un dato relevante).

Información del usuario

Este perfil de usuario está incompleto. Añade información de contacto de Alex sistemas, como una dirección de correo electrónico secundaria y un número de teléfono.

Privilegios y roles de administrador: Si el usuario tiene roles administrativos asignados, se mostrarán aquí, junto con la cantidad de privilegios que estos roles le otorgan.

Privilegios y roles de administrador	
Roles	Privilegios
Administrador de centro de asistencia, Administrador de Storage, Administrador de servicios, Administrador móvil	145 privilegios de la consola de administración, 5 privilegios de la API de administración

Nota Importante: Durante la implementación de la verificación en dos pasos, se decidió otorgar a todos los usuarios de la organización los roles que se visualizan en la presente imagen (Administrador de centro de asistencia, Administrador de servicios, Administrador de Storage, Administrador móvil). Esta asignación se realizó con la intención de proporcionar a los usuarios ciertos privilegios o capacidades específicas dentro de su entorno de Google Workspace, más allá del acceso básico a los servicios. Es importante revisar periódicamente si estos privilegios siguen siendo necesarios para todos y considerar alternativas más granulares para otorgar permisos específicos sin necesidad de roles de administrador completos.

DOCUMENTACIÓN

Roles			
Gestiona las funciones de administrador de Alex sistemas. Asigne funciones predefinidas o crea otras personalizadas con privilegios específicos.			
4 funciones asignadas			
Nombre del rol	Ámbito del rol	Estado de asignación ↑	Condición
Administrador de centro de asistencia Help Desk Administrator	Todas las unidades organizativas	Asignada	
Administrador de servicios Services Administrator	Todas las unidades organizativas	Asignada	
Administrador de Storage Storage Admin Role	Todas las unidades organizativas	Asignada	
Administrador móvil Mobile Administrator	Todas las unidades organizativas	Asignada	
Superadministrador Google Workspace Administrator Seed Role	-	Sin asignar	
Administrador de grupos Groups Administrator	-	Sin asignar	
Administrador de usuarios User Management Administrator	-	Sin asignar	
Lector de grupos Groups Reader	-	Sin asignar	-
Editor de grupos Groups Editor	-	Sin asignar	-
Administrador de Directory Sync Directory Sync Admin Role	-	Sin asignar	
Filas por página: 10 ▾		< Página 1 de 2 < >	

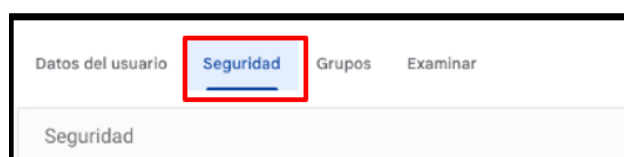
Aplicaciones: Un resumen de las aplicaciones de Google y otras aplicaciones en la nube que están activadas o disponibles para este usuario.

Aplicaciones		
Aplicaciones de Google 78 de los 79 servicios de Google disponibles están activados en la cuenta de Alex sistemas. Activar o	Otras aplicaciones en la nube No se han añadido más aplicaciones en la nube a esta organización. Buscar aplicaciones Activar o desactivar	Aplicaciones del Programa de Compra por Volumen (PCV) Alex sistemas utiliza 0 aplicaciones disponibles del

Esta página de Datos del usuario proporciona una visión general completa de la cuenta de un usuario y es el punto de partida para realizar diversas tareas de administración específicas para esa cuenta.

Paso 12. Para verificar el estado de la Verificación en dos pasos de un usuario específico, debemos acceder a la pestaña **Seguridad** de su perfil. Haz clic en la pestaña **Seguridad** ubicada junto a "**Datos del usuario**".

En esta sección, podremos observar la configuración de seguridad específica para este usuario.



DOCUMENTACIÓN

Se menciona la posibilidad de cambiar la contraseña del usuario desde aquí.

Seguridad	
Configuración de contraseña	
Contraseña	Puedes cambiar la contraseña de Alex sistemas.

Se informa si el usuario tiene llaves de seguridad registradas.

Llaves de seguridad	Alex sistemas no tiene llaves de seguridad	Más información
---------------------	--	---------------------------------

Protección Avanzada: Está **DESACTIVADA**. Se explica qué implica la Protección Avanzada y cómo activarla. También menciona la opción de utilizar un código de verificación alternativo si un usuario no puede iniciar sesión con su llave de seguridad.

Protección Avanzada	DESACTIVADO
Una vez que desactives el registro en la Protección Avanzada, solo el usuario podrá volver a registrarse. Más información	
Problemas para iniciar sesión	
Utiliza un código de verificación alternativo si un usuario no puede iniciar sesión con su llave de seguridad. Los códigos de verificación alternativos se pueden generar en la sección Verificación en dos pasos.	

Estado de la Verificación en dos pasos.

Verificación en dos pasos: Se explica que requiere un código adicional al iniciar sesión. Se muestra que tiene un teléfono de recuperación configurado y la opción de gestionar códigos de verificación alternativos.

Verificación en dos pasos	ACTIVADO	Se aplica en toda la organización
Esta opción permite a los usuarios iniciar sesión con un factor de autenticación adicional, además de su nombre de usuario y contraseña (p. ej., un código de verificación). Cambiar la configuración de seguridad		
Más información		
Obtener códigos de verificación alternativos		

Información de recuperación

En la sección **Información de recuperación**, se muestra el correo electrónico y el número de teléfono de recuperación configurados.

Información de recuperación	Correo electrónico
	Añadir una dirección de correo electrónico de recuperación
	Teléfono
	310 2533351
La información de recuperación se utiliza para proteger las cuentas de usuario en el inicio de sesión y durante la recuperación de una cuenta.	

Métodos de verificación del usuario.

Gestionar códigos de verificación alternativos permite generar códigos para situaciones donde el método principal no esté disponible.

Verificación en dos pasos

La verificación en dos pasos se aplica de forma obligatoria en tu organización

☒ Activado

☐ Desactivado

OBTENER CÓDIGOS DE VERIFICACIÓN ALTERNATIVOS

CANCELAR GUARDAR

Esta página permite verificar y gestionar la configuración de seguridad de un usuario específico.

4. Conclusión

En este manual, hemos recorrido paso a paso el proceso para configurar la Verificación en dos pasos a nivel organizacional dentro de la Consola del administrador de Google Workspace. Realizamos ajustes en la sección de Seguridad, estableciendo la obligatoriedad de esta capa de protección para todos los usuarios, definiendo cómo los nuevos usuarios deben adoptarla, gestionando la frecuencia con la que se solicita la verificación y configurando los métodos permitidos, incluyendo la opción de códigos de seguridad sin acceso remoto como medida de contingencia.

La implementación de la Verificación en dos pasos es una medida de seguridad fundamental en el entorno digital actual. Al requerir una segunda forma de verificación más allá de la contraseña, se reduce significativamente el riesgo de acceso no autorizado a las cuentas, protegiendo así la información sensible de la organización y la privacidad de los usuarios. Esta configuración proactiva fortalece la postura de seguridad general y ayuda a mitigar las amenazas comunes como el phishing y el robo de contraseñas.

Es importante recordar que la seguridad es un proceso continuo. Se recomienda revisar y actualizar periódicamente las políticas de seguridad, incluyendo la Verificación en dos pasos, para adaptarse a las nuevas amenazas y a las mejores prácticas en la industria. Comunicar claramente a los usuarios sobre la importancia de esta medida y brindarles el soporte necesario para su implementación también es crucial para el éxito de esta iniciativa de seguridad.