Más seguridad para tus usuarios: Implementación de 2FA

Hemos aplicado mejoras en el sistema de seguridad de doble factor (2FA) para nuestros usuarios. Esto fortalece significativamente el nivel de protección al acceder al software e información de tu empresa. Con esta actualización, garantizamos una capa adicional de seguridad que reduce el riesgo de accesos no autorizados.

¿Por qué es importante implementar un sistema de doble factor de autenticación?

La seguridad en el acceso a la información es fundamental para cualquier empresa, especialmente cuando se trata de datos sensibles. La autenticación de doble factor (2FA) añade una capa extra de protección al requerir un segundo método de verificación, además de la contraseña.

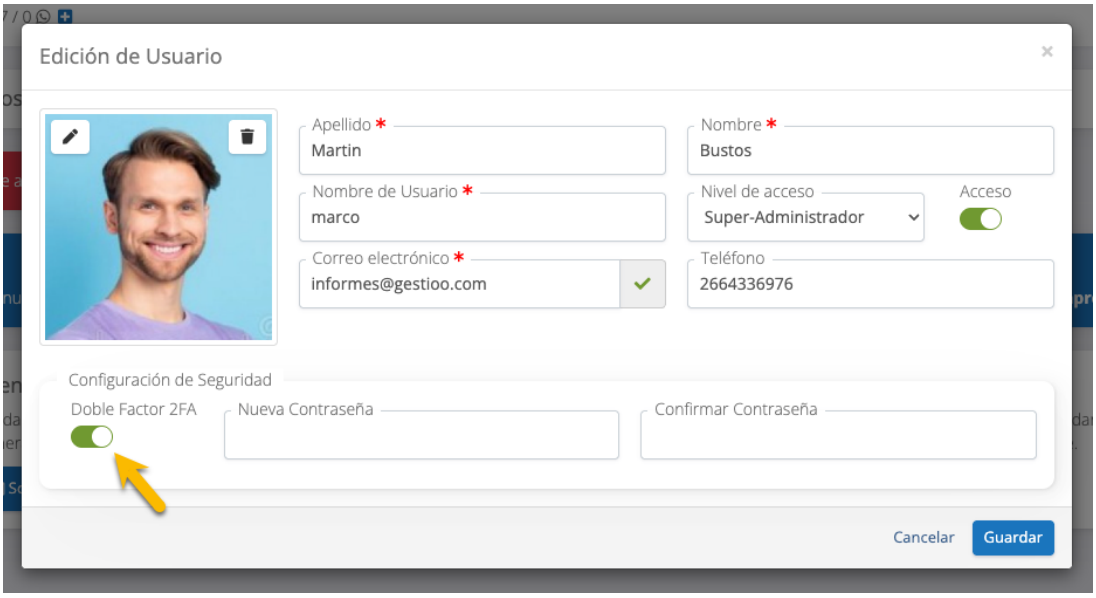
Algunas razones clave para implementar autenticación de doble factor son:

- **Prevención de accesos no autorizados**: Incluso si un atacante obtiene la contraseña de un usuario, no podrá acceder sin el segundo factor de autenticación.
- **Reducción de riesgos por contraseñas débiles o reutilizadas**: Muchas personas usan las mismas claves en varios servicios, lo que puede ser un riesgo si una de ellas se filtra.
- **Protección contra ataques de phishing y robo de credenciales**: Aunque un usuario sea víctima de un ataque de phishing, el código generado por la aplicación de 2FA impedirá que el atacante acceda.
- **Cumplimiento de normativas de seguridad**: En muchos sectores, la implementación de 2FA es un requisito de cumplimiento para garantizar la protección de los datos de clientes y empleados.

Activación del doble factor de autenticación en tu usuario

Para activar la autenticación de doble factor en tu cuenta, sigue estos pasos:

1. Dirígete a la edición de tu perfil de usuario. Activa la opción de seguridad 2FA y guarda los cambios.



2. Antes de cerrar la ventana, se te solicitará escanear un código QR con tu aplicación de autenticación 2FA e ingresar el código generado por dicha aplicación para completar el proceso.



3. Introduce el código generado por la aplicación en el campo correspondiente y haz clic en el botón “Confirmar”.



¡Listo! Ahora tienes configurado el doble factor de autenticación. A partir de este momento, cada vez que inicies sesión en el software, deberás ingresar el código 2FA generado por tu aplicación de autenticación.

¡Importante! Si no puedes escanear el código QR, puedes ver la clave de autenticación y copiarla manualmente en tu aplicación.



Configuración en la aplicación Authy

En **Gestioo**, recomendamos **Authy** (Authy.com) por su facilidad de uso, sincronización entre dispositivos y opciones de copia de seguridad, pero puedes elegir la aplicación de autenticación que mejor se adapte a tus necesidades.

Si deseas configurar el 2FA con Authy, sigue estos pasos:

1. Descarga e instala la aplicación **Authy** en tu dispositivo móvil. Enlace de descarga

2. Abre la aplicación y selecciona la opción **“Agregar cuenta”**.

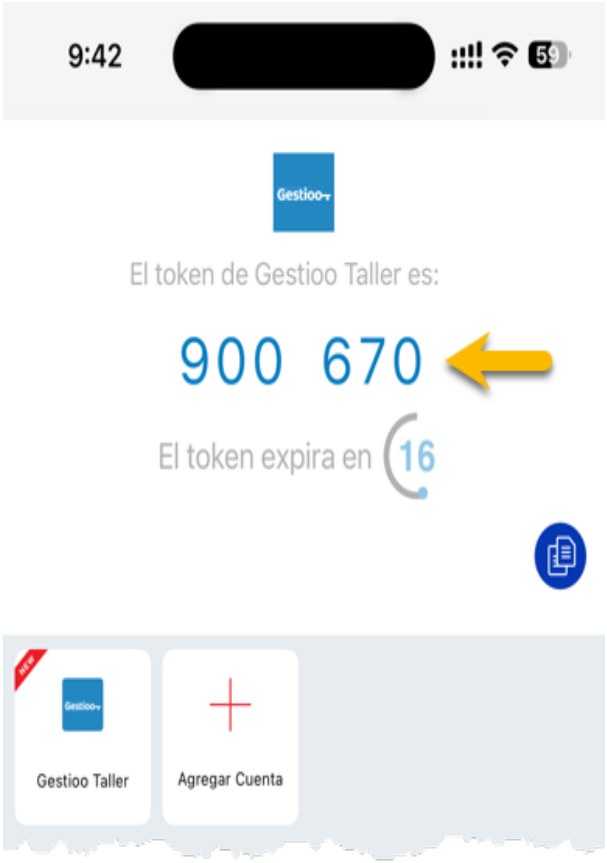


3. Pulsa en **“Escanear código QR”** y apunta la cámara de tu dispositivo al código QR que se muestra en la configuración del software.



4. Authy generará automáticamente una nueva cuenta con un código que cambiará cada ciertos segundos.

5. Guarda la cuenta y usa el código generado para completar la configuración en el software.



Authy ofrece la ventaja de sincronizar tus códigos entre dispositivos y realizar copias de seguridad cifradas en la nube, lo que facilita la recuperación de accesos en caso de pérdida del dispositivo.

Alternativas para gestionar tu 2FA

Existen diferentes aplicaciones y herramientas para gestionar códigos 2FA de manera segura. Aquí te dejamos algunas opciones recomendadas:

1. **Google Authenticator**: Aplicación sencilla y confiable que genera códigos 2FA sin conexión a internet, aunque no permite sincronización en la nube. Visitar sitio

2. **Microsoft Authenticator**: Compatible con una amplia variedad de servicios, ofrece la opción de copia de seguridad en la nube para restaurar los códigos en caso de cambio de dispositivo. Visitar sitio

3. **Bitwarden**: Además de ser un excelente gestor de contraseñas, Bitwarden incluye una función integrada de autenticación 2FA para administrar códigos de acceso en un solo lugar. Visitar sitio

La seguridad de la información es un pilar fundamental en cualquier empresa. Implementar un sistema de autenticación de doble factor (2FA) ayuda a reducir drásticamente los riesgos de accesos no autorizados y protege los datos de empleados y clientes.

Te recomendamos activar 2FA lo antes posible y fomentar su uso entre todos los miembros de tu equipo. Usar herramientas como **Bitwarden, Authy, Google Authenticator o Microsoft Authenticator** facilitará la gestión de códigos de autenticación de manera segura y eficiente.

Para una guía detallada sobre esta mejora de seguridad, no te pierdas nuestro video explicativo en YouTube, donde encontrarás un resumen completo de esta actualización.

Con estas mejoras en el sistema, ofrecemos una mayor tranquilidad a nuestros usuarios, asegurando que su información esté mejor protegida contra posibles amenazas cibernéticas. **¡Activa 2FA hoy y refuerza la seguridad de tu empresa!**

Etiquetas: 3.13, Seguridad, Usuarios