

## CIRCULAR Nº 200/2024

### ASUNTO:

“Doble factor”

#### **Ilmo./a. Sr./Sra.:**

Por medio de la presente, y para que confiera máxima difusión entre sus colegiados, le informamos que con objeto de fortalecer la seguridad en nuestras aplicaciones y en cumplimiento con el Esquema Nacional de Seguridad, a partir del próximo 25 de noviembre de 2024, se implantará un sistema de autenticación basado en doble factor en todas nuestras plataformas, incluyendo RAIA y RECEVET.

#### **¿Cómo funcionará el sistema de doble autenticación?**

1. **Acceso inicial:** Los usuarios seguirán introduciendo su usuario y contraseña como hasta ahora.
2. **Verificación adicional:** Tras introducir sus credenciales, se solicitará un código de seis cifras que se enviará por correo electrónico a la dirección registrada en su perfil.

### Introduzca código de doble factor

Se ha enviado un correo con un código de verificación a:  
fr\*\*\*\*\*@gm\*\*\*.com  
Introduce dicho código para continuar.

Tiempo restante: 04:25

[¿No has recibido el código? Enviar nuevo código](#)

3. **Validación del código:** El código tendrá una validez de cinco minutos. Si coincide con el enviado por correo electrónico, se permitirá el acceso a la aplicación; en caso contrario, se mostrará un mensaje de error y se regresará a la página principal.

### Configuración previa del correo para el doble factor

Antes de la fecha de activación, los usuarios podrán configurar el correo que se usará para el doble factor. Esto se hace accediendo a RAIA o RECEVET, en la opción “editar perfil” y seleccionando el correo deseado:

- **Múltiples correos registrados:** Los usuarios pueden marcar uno de los correos como el preferido para doble factor y, adicionalmente, designarlo como “de uso profesional”.
- **Eliminación de correos:** Los usuarios pueden eliminar los correos registrados, con la excepción del correo designado para el doble factor. Si desean eliminar este correo, primero deben marcar otro como correo de doble factor.

**Nota:** Si el usuario tiene solo un correo registrado, este se marcará automáticamente como el correo para doble factor.

### Selección del correo para doble factor el día de activación

El día de la activación, si en el perfil del usuario hubiera varios correos registrados, y no se hubiera seleccionado previamente cual se usará para el doble factor, se solicitará que seleccione uno para la autenticación. Una vez seleccionado, se pedirá nuevamente el usuario y contraseña, seguido del código de doble factor.



No existe email marcado para doble factor,  
debe elegir uno

fr\*\*\*\*\*@gm\*\*\*.com

mo\*\*\*\*\*@ho\*\*\*\*\*.com

Aceptar

### En caso de no tener un correo registrado

Si en la fecha de activación no hay ningún correo en el perfil del usuario, se mostrará el siguiente mensaje:

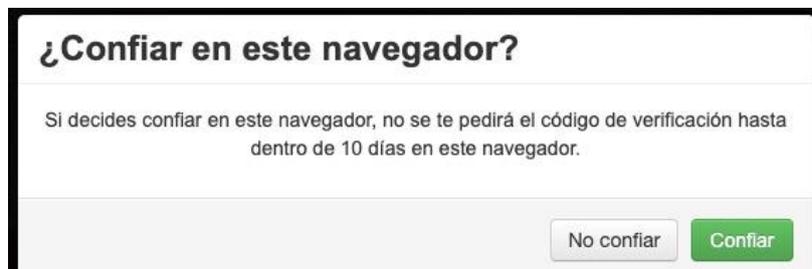


**Consejo Andaluz de Colegios Oficiales de Veterinarios**  
Calle Gonzalo Bilbao, nº 23-25 bajo.  
41003. Sevilla.

“No tiene emails que puedan usarse para enviarle el doble factor de autenticación. Por favor, comunique un correo electrónico válido a través de la ventanilla única del Consejo Andaluz de Colegios Oficiales de Veterinarios, utilizando un certificado digital.”

### **Uso de navegadores de confianza**

A partir de la activación, al introducir usuario y contraseña, aparecerá una opción para “confiar en este navegador por 10 días”. Si se selecciona, el sistema no volverá a solicitar el doble factor en ese navegador durante ese periodo.



Al cerrar sesión, si el usuario había marcado el navegador como confiable, se le preguntará si desea seguir confiando en él. Si responde “Sí”, el sistema no solicitará el doble factor al iniciar sesión dentro del periodo de confianza de diez días. En caso de responder “No”, el sistema volverá a pedir el doble factor la próxima vez que inicie sesión en ese navegador.

Departamento de Informática  
Consejo Andaluz de Colegios Oficiales de Veterinarios.

**ILMO/A. SR./SRA. PRESIDENTE DE COLEGIO VETERINARIO.**