

Para garantizar una conexión segura desde los sitios públicos wifi se han implementado certificados de seguridad acordes con los estándares internacionales en el Portal de autenticación *nauta* y en los navegadores que se utilizan con frecuencia en los diferentes dispositivos. No obstante, usted debe tener en cuenta las siguientes recomendaciones para mayor seguridad:

- **Conéctese solamente a la red inalámbrica WIFI\_ETECSA** en los espacios públicos declarados como sitios wifi.
- **Conéctese siempre como usuario de ETECSA** y no a través de otras personas o aplicaciones para abaratar la conexión. Esto afecta su calidad y expone su seguridad.
- **No se conecte cuando aparezcan ventanas con advertencia de seguridad** alertando que existen problemas con el certificado del sitio. Es posible que algunas personas intenten robar sus credenciales (usuario y contraseña). Ante esta situación intente conectarse nuevamente solo cuando se muestre el portal sin notificaciones previas.
- **No comparta sus credenciales (usuario y contraseña) con extraños.** Pueden hacer uso indebido y no autorizado de las mismas.
- **No guarde las credenciales en su equipo** y no preste los dispositivos con los que suele conectarse.
- **Cambie periódicamente la contraseña** en el PORTAL DE USUARIO.
- **No acepte propuestas de transferencia de saldo de desconocidos** en los sitios wifi pues pudiera estar asociado a robos de cuentas de otros usuarios y verse involucrado en la investigación por fraude.
- **Elimine los datos de su navegador (cookies, caché, certificaciones, etc.)** cada vez que se conecte.
- **Solicite el “reseteo” o “bloqueo” de su cuenta *nauta* de acceso permanente a través del 118**, en caso de que se muestre la notificación “*Su cuenta está en uso*” antes de autenticarse.

Ante la evidencia de pérdida de saldo no justificado por sus acciones de navegación, llame al 118 o reclame en la unidad comercial más cercana.

ETECSA no solicita credenciales para ofrecer sus servicio. Éstas son de carácter privado y confidencial, por lo que le reiteramos no compartir sus credenciales con extraños.

***¡Recuerde que usted es el responsable de la seguridad de su cuenta!***

## **Preguntas Frecuentes**

1. ¿El Portal de autenticación garantiza una conexión segura?

Sí. Nuestro portal *nauta* tiene implementado certificados de seguridad acordes con los estándares internacionales.

2. ¿Todos los navegadores cuentan con certificados de seguridad?

Sí. Todos los navegadores reconocen los certificados válidos.

3. ¿El Portal de usuario nauta garantiza una conexión segura?

No. El portal de usuario *nauta* aún no cuenta con un certificado válido.

4. ¿Cómo puedo saber si el portal es seguro?

El portal es seguro si al establecer conexión le aparece en la dirección URL que está usando *https* y si no le sale una alerta/advertencia de seguridad indicando que el certificado de seguridad no es válido o la conexión no es segura.

5. ¿Qué debo hacer en caso de que se muestre una advertencia de seguridad?

No debe acceder a través de esta ventana. Intente conectarse nuevamente cuando se muestre el portal **nauta** sin notificaciones previas.

6. ¿Puede aparecer alguna advertencia de seguridad en las salas de navegación?

No. Nuestro portal de autenticación **nauta** tiene implementado certificados de seguridad acordes con los estándares internacionales.

7. ¿Existe alguna otra forma de que roben mis credenciales (usuario y contraseña) que no sea a través de las ventanas con advertencia de seguridad?

Sí. Es por eso que le recomendamos:

- Conectarse solamente a la red inalámbrica WIFI\_ETECSA en los espacios

- públicos declarados como sitios wifi.
- Conectarse siempre como usuario de ETECSA y no a través de otras personas o aplicaciones para abaratar la conexión. Esto afecta su calidad y expone su seguridad.
- No conectarse cuando aparezcan ventanas con **advertencia de seguridad** alertando que existen problemas con el certificado del sitio. Es posible que algunas personas intenten robar sus credenciales (usuario y contraseña). Ante esta situación intente conectarse nuevamente solo cuando se muestre el portal al que desee acceder, sin notificaciones previas.
- No compartir sus credenciales (usuario y contraseña) con extraños. Pueden hacer uso indebido y no autorizado de las mismas.
- No guardar las credenciales en su equipo y no preste los dispositivos con los que suele conectarse.
- Cambiar periódicamente la contraseña en el PORTAL DE USUARIO.
- No aceptar propuestas de transferencia de saldo de desconocidos en los sitios wifi pues pudiera estar asociado a robos de cuentas de otros usuarios y verse involucrado en la investigación por fraude.
- Eliminar los datos de su navegador (cookies, caché, certificaciones, etc.) cada vez que se conecte.
- Solicitar el “reseteo” o “bloqueo” de su cuenta *nauta* de acceso permanente a través del 118, en caso de que se muestre la notificación “*Su cuenta está en uso*” antes de autenticarse.

8. ¿Puedo acceder a sitios que muestren advertencias de seguridad?

Solo al del **Portal de usuario *nauta***, ya que este aún no cuenta con un certificado válido. Le sugerimos no acceder a ningún otro sitio que muestren alertas de seguridad.

9. ¿Cómo puedo eliminar los datos (cookies, caché, certificados, etc.) de mi navegador?

Debe ir a los *Ajustes* de su navegador y elegir las opciones de *borrar caché, datos de cookies, etc.*

10. ¿Qué pasa si no elimino los datos (cookies, caché, certificados, etc.) de mi navegador?

Puede almacenar certificados de seguridad de sitios falsos a los cuales ya accedió una vez, y correría el riesgo de volver a conectarse sin recibir alertas de seguridad y que otro usuario obtenga sus credenciales.

11. ¿Qué son las cookies?

Las «Cookies» son pequeños archivos usados por los sitios webs para almacenar información en el dispositivo (como información para iniciar sesión y las preferencias de un sitio).

12. Si elimino las cookies de mi navegador ¿Se elimina también el historial?

No.

13. ¿ETECSA solicita el usuario y la contraseña para brindar algún servicio?

No. ETECSA nunca solicitará sus credenciales para ofertar ningún servicio.

14. Yo me he conectado a través de los llamados “Conected 5” ¿Esto puede comprometer la seguridad de mi cuenta?

Sí. Le sugerimos conectarse siempre como usuario de ETECSA y no a través de otras personas o aplicaciones para abaratar la conexión. Pueden hacer uso indebido de sus credenciales y comprometer la seguridad de su cuenta.

15. ¿Qué debo hacer si anteriormente he sido víctima de algún fraude de este tipo?

Le sugerimos eliminar todos los datos de su navegador (cookies, certificados, caché) y cambiar periódicamente su contraseña.

16. ¿Qué puedo hacer si aparece una ventana donde se muestre: “Su cuenta está en uso” sin haberme autenticado?

Debe llamar al 118 y solicitar el reseteo o bloqueo de su cuenta.

17. ¿Para qué sirve el reseteo?

El reseteo permite reiniciar su cuenta. De esta forma, se cerraría la sesión en caso de que su cuenta estuviera en uso, y la persona que estuviera utilizando sus credenciales tendría que autenticarse nuevamente. Es por ello que le sugerimos, una vez realizado el reseteo, cambiar inmediatamente su contraseña en el Portal de usuario para evitar que vuelvan a utilizar sus credenciales.

18. ¿Qué sucede si solicito el bloqueo de mi cuenta?

En este caso su cuenta no podrá ser usada hasta que el titular solicite el desbloqueo de la misma directamente en la unidad comercial.

19. ¿Qué debo hacer ante la pérdida de saldo no justificado?

Le sugerimos acudir a la oficina comercial más cercana o llamar al 118.