



INFÓRMATE MÁS ACERCA DE LA

SEGURIDAD DE LA INFORMACIÓN

www.rentanacional.cl

INFÓRMATE MÁS ACERCA DE LA **SEGURIDAD DE LA INFORMACIÓN**

Renta Nacional toma diferentes medidas para proteger la información de todos nuestros clientes. Sin embargo, las acciones de los clientes también juegan un papel importante en la protección de sus datos.

Proteger tu información personal ayuda a reducir el riesgo de delitos relacionados a la suplantación de identidad y utilización ilegal de datos personales. Para el resguardo de tu información, Renta Nacional le aconseja tomar las siguientes medidas de seguridad:

¿CÓMO PUEDES PROTEGER TU INFORMACIÓN?

TE ACONSEJAMOS:

01 Consultar siempre a través de los canales oficiales que mantiene la compañía para compartir tu información personal.

- Sitio web: <https://seguros.rentanacional.cl/>
- Call Center: 800 200 050 / +562 2670 0202
- Correo electrónico: servicioalcliente@rentanacional.cl
- Aplicación Google Play o App Store: Renta Nacional
- Ejecutivo Comercial

02 Almacenar tu información personal de forma segura, especialmente tu contraseña datos personales.

03 Si deseas eliminar información que posee tus datos personales, debes asegurarte de no dejar rastro alguno en los documentos que contengan estos datos.

04 Si recibes un llamado, asegúrate de que corresponda al número oficial de la compañía:

 **+562 2670 0202**



ELIJE UNA CONTRASEÑA SEGURA

- 01** Elije una contraseña que sea fácil de recordar para usted, pero difícil de adivinar para los demás.
- 02** Cuando sea posible, usa una frase de contraseña, procura que sea lo más larga posible sin usar frases comunes e incluye caracteres, números y letras mayúsculas y minúsculas. Por ejemplo: ElTítuloDeTuCanciónFavorita#05.
- 03** No utilices la misma contraseña para diferentes cuentas o servicios en línea.
- 04** Cambia tus claves, al menos una vez al año.
- 05** Las contraseñas deben ser secretas y únicas, no debes compartirlas por correo electrónico ni mensajes de texto.
- 06** Cuida que nadie te observe cuando las digites, no habilites la opción de guardar contraseña en el navegador que utilizas, ni en tu dispositivo móvil.
- 07** Nunca guardes las contraseñas en tu correo personal, en el bloc de notas de tu celular o en un papel que sea visible por terceros.
- 08** Algunos consejos:
 - No utilizar su nombre, o el nombre de algún familiar.
 - No utilizar el nombre de alguna mascota.
 - No utilizar fechas de cumpleaños.
 - No usar direcciones del trabajo o domicilio particular
 - No usar el RUT personal o de algún familiar
 - No usar el número de teléfono



PROTEJE TUS NÚMEROS DE CUENTA Y CONTRASEÑAS

Nunca compartas tus nombres de usuario o contraseñas con nadie. Ten cuidado con los correos electrónicos o las personas que solicitan esta información. Nunca solicitaremos tu contraseña personal por correo electrónico o por teléfono.

Si necesitas anotar la información de inicio de sesión, guárdala en un lugar seguro. No lles esta información en tu billetera.

PROTEJE TU COMPUTADORA PERSONAL Y DISPOSITIVOS MÓVILES

TU COMPUTADORA PERSONAL

Tu computadora y dispositivos móviles están expuestas a toda la información que le sirve a los ciberdelincuentes para robar su identidad. Esto incluye los programas y Computadora, tablets, celulares, consolas de videojuegos e incluso televisiones inteligentes.

Es por esto que debemos mantener la seguridad de nuestros dispositivos con los siguientes consejos:

- Mantener el equipo actualizado.
- Proteger su equipo con antivirus
- Ser cuidadosos con las aplicaciones que instalamos, huyendo de fuentes no confiables y vigilando los privilegios que les concedemos.

TUS DISPOSITIVOS MÓVILES

No te olvides que tu celular y tablet son tan importantes como una computadora personal. Para eso le aconsejamos lo siguiente:

- Activa siempre un PIN o una función de bloqueo para su dispositivo.
- Evita instalar aplicaciones fuera de las tiendas de aplicaciones de Apple o Google Store. Algunas aplicaciones pueden contener malware diseñado para robar tu información personal y financiera.
- También es una buena idea leer las reseñas y los comentarios de otros usuarios para ver si se ha informado algo sospechoso sobre la aplicación.


En caso de pérdida o hurto de alguno de sus dispositivos móviles, te aconsejamos cerrar las aplicaciones y cambiar tu clave.



MEDIDAS DE PROTECCIÓN AL NAVEGAR

Sigue las siguientes recomendaciones:

- Conectarse a red wifi con contraseña segura.
- Evita conectarse en wifi públicas.
- Nunca guardes tu contraseña en el navegador.
- Cerrar sesión en las aplicaciones y navegador web después de haberlas utilizado.
- Revisa las URL y verifica que el sitio corresponda al que quieres ingresar. Si no coincide, **NUNCA** ingreses tus datos personales.
- Verifica que el sitio web tenga el candado de seguridad. Esto asegura que la información está cifrada y sólo accederá a tus datos el destinatario.

 Esta página web no corresponde al sitio oficial de renta nacional y hemos detectado que presuntamente está siendo mal utilizado: **<https://renta-nacional.com/>**



OTROS

- Desconfiar de quienes solicitan depósitos.
- No Transferencias a personas naturales.
- Verifique que sea una entidad regulada.
- Verificar alertas ciudadanas que entrega la CMF.
- Ante dudas, verifique siempre la página de la CMF.
- Verifique la redacción y ortografía de quien lo contacte.

PROTÉGETE DE LAS REDES SOCIALES

Evita publicar:

- Información personal (domicilio, número de teléfono, fechas importantes, Rut, entre otros)
- Información financiera
- Locación y período de vacaciones
- Asegúrate de que tus contactos en las redes sociales son realmente quienes crees que son. No nos conformemos con ver la foto, el nombre o que es amigo de nuestros amigos.





IMPORTANTE

Si experimentas fraude o sospecha una violación de una cuenta debes dar aviso al siguiente correo:



ciberdenuncias@rentanacional.cl



INFÓRMATE MÁS ACERCA DE LA
SEGURIDAD DE LA INFORMACIÓN

www.rentanacional.cl