



# Políticas de seguridad

## Así te protegemos

Para nosotros tu información personal y las operaciones que realizas en nuestro sitio son de suma importancia, por lo que implementamos estrictas medidas de seguridad para proteger tu información, asegurando: confidencialidad, disponibilidad e integridad de la operatoria a través de Internet. Las principales medidas de seguridad que implementamos para protegerte de accesos NO autorizados son las siguientes:

## Seguridad en la clave de acceso

Es necesario que previo a acceder a funciones monetarias, sean estas de consulta (ejemplo: visualización del resumen) o transaccionales (ejemplo: Recarga de celulares) por medio de nuestro sitio te identifiques con un usuario y una clave de identificación personal (clave). Las características de esta última cumplen con lo exigido por el BCRA Comunicación A 4609 referente a estándar de acceso, de identificación y autenticación y reglas de seguridad (bloqueo ante intentos de acceso fallidos, tiempo límite de inactividad, etc.)

## Disponibilidad del servicio

Contamos con planes de contingencias y continuidad de operaciones para los servicios que te ofrecemos por medio de Internet. Nuestro sitio se encuentra disponible los 365 días del año.

## Cifrado de datos

Utilizamos técnicas de encriptación de datos (proceso de conversión que transforma los datos en una secuencia de datos únicos e ilegibles) para que tanto el canal de transmisión de información como el almacenamiento sean seguros. De esta manera evitamos que terceros puedan ver lo que haces o qué información envías y recibís desde nuestro sitio.

## Seguridad Física

Nuestros activos críticos (servidores, equipos de comunicaciones, etc.) relacionados con la operatoria web, se encuentran convenientemente resguardados. Nuestros centros de cómputos cuentan con efectivas medidas de seguridad en función a las buenas prácticas y normativas de B.C.R.A.

## Firewalls e IDS

Aplicamos medidas de seguridad para delimitar nuestra red interna y externa, y de esta forma controlar la no existencia de intromisiones indeseadas a nuestros sistemas internos.

Utilizamos firewalls para analizar y filtrar conexiones no deseadas que llegan a nuestros servidores. Adicionalmente contamos con un sistema de detección y prevención de intrusos, el cual actúa en forma preventiva y elimina los riesgos de intromisión, monitoreando en tiempo real nuestra red buscando posibles ataques.

A su vez contamos con Sistemas de Detección de Virus. Desde AssistHome poseemos registros de las actividades que realizas en nuestro sitio a modo de monitoreo.

## Certificados de seguridad

[www.AssistHome.com.ar](http://www.AssistHome.com.ar) es un sitio web seguro, utilizamos tecnología y mecanismos completos y eficaces.



## Protégete a ti mismo

Te recomendamos que no dejes tu información personal al descubierto, para que no pueda ser accedida por malintencionados.

Nunca respondas a correos electrónicos inesperados o de origen sospechoso y NO hagas click en enlaces o archivos adjuntos en mensajes de este tipo.

Existen ataques llamados phishing que ocurren cuando malintencionados engañan a los usuarios creando una identidad falsa para solicitar contraseñas o información de de crédito. Al respecto, sé sumamente cauto y responsable sobre la información que brindas y recuerda que AssistHome nunca te solicitará develar tu contraseña.

Acostúmbrate a cerrar la sesión del sitio, principalmente cuando accedes desde computadoras que son utilizadas por varias personas (ej. cyber). De lo contrario, puede que la sesión permanezca disponible para ser utilizada por otras personas.

Es importante que mantengamos tus datos actualizados en nuestra base de datos en caso de que tengamos que comunicarnos para confirmar detalles.

Es importante mencionar que siempre que detectes irregularidades en tu información vinculada con la operatoria del sitio nos informes enviando un correo a: [repcion@AssistHome.com.ar](mailto:repcion@AssistHome.com.ar), o llamando a nuestros asesores: 0810-220-0059 (las 24 horas)

## Protege tu computadora

Si tu computadora está afectada de virus, tu información personal y financiera puede estar comprometida, por lo que te recomendamos que instales un software de antivirus y lo actualices periódicamente. Este también te ayudará a prevenir el spyware (software malicioso que monitorea las actividades de tu computadora, tales como detalles de contraseñas o sitios web que has visitado).

También te recomendamos que actualices las versiones de tu navegador de internet evitando contar con vulnerabilidades de seguridad. Siempre mantené el firewall de tu computadora activo ya que previene el posible acceso de los usuarios no autorizados a tu información personal.

Elige una contraseña segura

La mejor contraseña es la que te resulta fácil de recordar pero imposible de adivinar para cualquier otra persona. A continuación te recomendamos que hacer para que tu contraseña sea segura:

- Nunca compartas tus contraseñas con nadie. Y nunca debes escribir tus contraseñas o almacenarlas en tu computadora.
- Te recomendamos que utilices letras de una frase o una canción. La mezcla de mayúsculas y minúsculas con números, ayuda a que la contraseña sea más segura.
- No uses tu PIN o reutilices las contraseñas de otros canales.
- No utilices nombres de familiares o fechas de cumpleaños porque son fáciles de adivinar para los atacantes, especialmente si utilizas tu propio nombre o fecha de cumpleaños.
- No utilices palabras de diccionario porque los atacantes suelen usar los diccionarios de contraseñas de uso común. Evita contraseñas que contengan palabras reales, nombres o palabras en idiomas extranjeros.
- No mal deletrees palabras comunes, los atacantes están dispuestos a probar estas combinaciones, así, sobre todo las secuencias que sustituyen letras como la I con un 1 o E con el 3.



## Seguridad Wireless

En la actualidad podés acceder a Internet desde cualquier lugar y en el momento que quieras, ya que las redes wireless están disponibles en todos lados, pero como ésta conexión se genera por ondas de radio y no por cables, hace que tu computadora sea más vulnerable a los ataques. Por lo que te recomendamos:

- Comprueba que la red wireless esté protegida para detener a los atacantes.
- Asegurate de tener un firewall activado.
- Elige una password SEGURA para la red wireless.

## Seguridad en tu celular

Te recomendamos que antes de instalar una aplicación en tu dispositivo, revises los permisos que requiere y que los mismos sean pertinentes a las funciones que brinda la misma.

## Sitios vinculados

Este sitio puede brindar acceso a información suministrada por terceros o vínculos a otras direcciones de internet, que no son mantenidos ni se encuentran bajo la responsabilidad de AssistHome . Esta última no se responsabiliza por el contenido de aquellos sitios. La inclusión de algún vínculo a los mencionados sitios no implica aprobación o aval de los mismos o del contenido disponible en los sitios. AssistHome , no controla ni garantiza, ni asume responsabilidad alguna por la exactitud, la oportunidad o inclusive la disponibilidad continua de los mismos. La responsabilidad por el acceso a los sitios vinculados es exclusiva del Usuario.

Domicilio legal de Worlybaires S.A CUIT 30-71043007-8  
Alsina 756 5A, Ciudad Autónoma de Buenos Aires, Argentina