

1. Borrado digital

Este servicio permite solicitar la cancelación de los datos personales de los Asegurados que aparezcan en páginas de Internet siempre con sujeción a la legislación vigente en cada momento. Para poder prestar el servicio el Asegurado deberá facilitar instrucciones por escrito de las tareas a realizar, debidamente firmadas, y copia de su DNI. Entre otras, se incluye la solicitud de cancelación a:

- Redes sociales
- Redes profesionales
- Blogs
- Webs de cualquier tipo que alberguen información personal
- Cuentas de correo electrónico

A solicitud del usuario ALMUDENA realizará un rastreo previo para detectar las páginas web en las que aparezca información personal. No se tendrán en consideración las páginas web correspondientes a medios de comunicación. El usuario del servicio deberá indicar a ALMUDENA las páginas web en las que desea que se cancelen sus datos personales.

En caso de negarse la página web a cancelar la información personal, se informará al Asegurado sobre las opciones existentes pudiendo optar por una reclamación de carácter jurídico, la denuncia ante la Agencia de Protección de Datos en caso de resultar factible o una gestión de otro tipo.

Un borrado por anualidad de seguro.

Exención de responsabilidad

En función de diferentes características de la página web, como el país donde se ubique la empresa que la gestiona o la transparencia de sus responsables, puede no resultar eficaz nuestro servicio por lo que no se garantiza la obtención de resultado alguno.

2. Mejoras Asistencia Tecnológica

Gestión de Contraseñas seguras

Previa petición por parte del Beneficiario, **se** gestionará a través de conexión remota la descarga e instalación de un programa informático para ordenadores personales que permita gestionar las contraseñas del usuario y realice una validación de la seguridad de las contraseñas utilizadas.

Control Parental

El Asegurado podrá solicitar la configuración de una cuenta de usuario específica para gestionar y filtrar los contenidos de Internet a los que pueden acceder los menores cuando estén utilizando un dispositivo informático, con conexión a Internet, sin supervisión de un adulto.

Las principales funcionalidades que se pueden configurar son:

- Limitación de acceso a determinados contenidos.
- Limitación en el tiempo de conexión.
- Establecimiento de una banda horaria para la conexión.
- Reporte de webs visitadas.
- Reporte de conversaciones por chat.
- Reporte de envíos por e-mail.
- Control de programas y juegos que pueden usar.
- Bloqueo del acceso a películas y programas de TV inapropiados.

La eficacia de este servicio está limitada por las características tecnológicas de cada tipo de dispositivo.

Protección ante vulnerabilidades

Previa petición del Beneficiario, **se** prestará un servicio de auditoría para la evaluación del nivel de riesgo tecnológico asociado a los sistemas y plataformas TIC expuestos como servicios públicos en Internet, basado en la detección de vulnerabilidades conocidas de carácter público.

El servicio se desarrolla a partir de una plataforma de gestión de seguridad alimentada a partir de las principales bases de datos existentes de vulnerabilidades reconocidas por los distintos fabricantes de tecnología TIC.

Se establece un límite de un servicio a una dirección IP al año.

Protección y mejoras de redes wifi

A solicitud del Asegurado se prestará un servicio de Protección y optimización de redes wifi que incluirá las siguientes prestaciones:

1. Análisis y detección, en su caso, de conexiones no autorizadas a la red wifi del Asegurado.
2. Consejos de optimización de la red wifi.
3. Revisión de la seguridad y configuración de la red del Asegurado.
4. Pruebas de rendimiento.
5. Instalación de un programa que permita controlar futuros accesos no autorizados a la red wifi del Asegurado.

La red wifi debe estar instalada en el hogar/comercio/empresa objeto del seguro en el que se incluya esta prestación.

Queda excluido el servicio en los siguientes casos:

1. **Ausencia de conexión a internet plena y estable.**
2. **Asistencia a redes de las que no se disponga de los datos necesarios para la configuración del router/modem.**
3. **Redes con conexión indirecta al router (AP, PLC, Servidores, Ruteadores, Switches, etc.)**

El Asegurador no se hace responsable de posibles ataques o conexiones fraudulentas a la red una vez optimizada y configurada.