**¿Que es telegram?**

Telegram es un servicio de mensajería por Internet desarrollado por los hermanos [Nikolai](http://es.wikipedia.org/w/index.php?title=Nikolai_Durov&action=edit&redlink=1" \o "Nikolai Durov (aún no redactado)) y [Pavel Durov](http://es.wikipedia.org/wiki/Pavel_Durov), creadores de la red social VK. Fue estrenado en el 2013 después que el fundador Pavel Durov anunciara su salida laboral de VK; inicialmente fue empleado para teléfonos móviles y el año siguiente para multiplataforma. Dicho servicio consiste en enviar y recibir mensajes (sea texto, documentos o miscelánea) a través de la arquitectura [MTProto](http://es.wikipedia.org/wiki/MTProto" \o "MTProto), desarrollada por ellos mismos, en lugar de la popular XMPP.

Desde el 2013 el proyecto —sin ánimo de lucro e independiente de VK— tiene como sede en Berlín y es operado de manera gratuita tanto su protocolo API como sus clientes operativos. Con la obtención de clientes oficiales —para los sistemas operativos móviles [Android](http://es.wikipedia.org/wiki/Android), [iOS](http://es.wikipedia.org/wiki/IOS_(sistema_operativo)) y Windows Phone, así como ordenadores y aplicaciones web— se emplearon otras utilidades bajo el concepto de software libre (excepto el lado del servidor) que pueden ser modificados por la comunidad.

Como un servicio para emisión y recepción de escritos, ubicaciones por GPS, imágenes estáticas, animaciones o videos de alta duración, Telegram ofrece características con mayor soporte. Entre ellas: La interacción de archivos multimedia, búsqueda global (que comprenden archivos multimedia, videos, e historial), salas grupales, y el uso de chats secretos (que establecen mutuamente un límite de duración y disponibilidad). De acuerdo al lema de proveer mayor privacidad y seguridad, las aplicaciones sufrieron cambios de diseño y facilidad de manejo.

Fue traducido al español para los móviles a principios de febrero de 2014 y para computadoras a finales del mismo año. Tras una falla en el sistema de [WhatsApp](http://es.wikipedia.org/wiki/WhatsApp) el 24 de febrero de 2014 Telegram aumentó sorpresivamente su cuota de uso en España y otros países, llegando a ser uno de los competidores más influyentes de la mensajería instantánea.

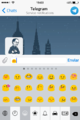
**Características**

El énfasis en la seguridad y privacidad fue como respuesta al [proyecto de vigilancia electrónica PRISM](http://es.wikipedia.org/wiki/PRISM). Para las tareas de sincronización y gestión de mensajes tanto de envío como de recibo se utiliza la [computación en la nube](http://es.wikipedia.org/wiki/Computaci%C3%B3n_en_la_nube), que puede involucrar a varios dispositivos. El sistema soporta documentos, multimedia, notas de audio, zonas geolocalizadas, [GIFs](http://es.wikipedia.org/wiki/GIF" \o "GIF), contactos, enlaces web, y otros archivos con un máximo de 1.5 [gigabytes](http://es.wikipedia.org/wiki/Gigabyte) cada uno. Estos datos pueden son almacenados en el historial de forma privada y ser buscada cualquier palabra o frase. Además incluye una galería multimedia sin necesidad de realizar una lectura o descarga completa de archivos en el dispositivo. Para la interacción del contacto, se muestra un estado: si escribe, envía una foto, comparte un vídeo o sube un archivo antes de compartirlo.

También se incluyen otras utilidades, algunas opcionales o implementadas en la arquitectura en la nube [MTProto](https://es.wikipedia.org/wiki/MTProto" \o "MTProto):

[](https://commons.wikimedia.org/wiki/File:Telegram_Giphy_search.PNG)

Buscador de imágenes y animaciones, uno de los añadidos de Telegram.

[](https://commons.wikimedia.org/wiki/File:Telegram_Sticker.PNG)

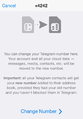
Stickers, usando desde el teclado a Steve Jobs, otro añadido externo.

[](https://commons.wikimedia.org/wiki/File:Telegram_Sesiones_activas.png)

Página de sesiones activas, con la posibilidad de añadir una contraseña de acceso.

[](https://commons.wikimedia.org/wiki/File:Telegram_Primer_Registro.png)

Confirmación de un número telefónico al registrarse o iniciarse por primera vez.

[](https://commons.wikimedia.org/wiki/File:Telegram_migration.png)

Migración de número a otro; los contactos y el historial son conservados en la nube.

**Añadidos externos:** A finales de 2014 se integró un buscador para encontrar imágenes por [Internet](http://es.wikipedia.org/wiki/Internet) y conservarlos en la lista "Reciente". De forma paulatina, usando la base de datos de [Giphy](http://es.wikipedia.org/w/index.php?title=Giphy&action=edit&redlink=1" \o "Giphy (aún no redactado)), se implementó al servicio una colección de cortos animados o [escenas virales](http://es.wikipedia.org/wiki/Fen%C3%B3meno_de_Internet) (en formato GIF) para escoger desde la aplicación para iOS y, días después, los dispositivos Android. A inicios de 2015 las aplicaciones pueden usar los [stickers](http://es.wikipedia.org/wiki/Pegatina" \o "Pegatina) que se relacionan con los emoticonos.

**Conexión y lectura:** Los contactos e invitados pueden saber si el usuario está conectado en línea o la última vez que estuvo en el programa; con la opción de cambiar a "ocasionalmente" o "hace mucho tiempo" en la sección "Privacidad".Para las conversaciones, las [marcas de verificación](http://es.wikipedia.org/wiki/Visto) son indicadas debajo del cuadro de texto: Uno ([Check](http://commons.wikimedia.org/wiki/File:Blue_check_PD.svg)) cuando el mensaje es enviado a la nube con éxito; y dos ([CheckCheck](http://commons.wikimedia.org/wiki/File:Blue_check_PD.svg)) cuando el receptor terminó de leer una vez recibido.

**Chats secretos:** Siempre que el otro usuario acepte la invitación, se abre una sesión de chat por separado, cuyos mensajes son transmitidos mediante una clave de cifrado y decodificado en dispositivos de extremo a extremo. Las claves son renovadas cuando se termina la conversación y los mensajes se desvanecen cuando son leídos un cierto tiempo. En octubre de 2014 se incluyó el modo "toca y suelta" para las imágenes con la posibilidad de autodestruírse.

**Confirmación de número telefónico:** Si el número se asigna a la aplicación por primera vez, se enviará un código por [SMS](http://es.wikipedia.org/wiki/Servicio_de_mensajes_cortos) o llamada telefónica sin gastos de envío. A partir del siguiente dispositivo instalado, la dirección IP y la hora de solicitud, seguido del código de seguridad, será enviado directamente a los ya asignados.

**Identificación por alias:** Cada usuario puede identificar su propio número con un [alias](http://es.wikipedia.org/wiki/Alias), de la misma manera que se realiza con una [cuenta de usuario](http://es.wikipedia.org/wiki/Cuenta_de_usuario). Así, el receptor podrá buscar e identificar por el alias, el nombre del receptor y su imagen de perfil, sin necesidad de tener agregado en sus contactos ni revelar su número. Desde diciembre de 2014 se creó un acceso directo tipo *telegram.me/minombre*.

**Lista de difusión y grupos:** En una actualización de agosto de 2014 el usuario tiene la posibilidad de enviar un mensaje a varios contactos a la vez, siempre que tengan añadido el número del emisor, mediante una lista personal, tanto para ahora como para futuros usos. Para realizar conversaciones unificadas, los participantes pueden formar grupos de hasta 200 usuarios, con un nombre y un historial aparte, con la posibilidad de invitar a otros contactos.

**Transferir usuario a otro número:** Mediante la opción *Cambiar número*, se puede migrar la cuenta de usuario a otra línea telefónica conservando los mensajes e información de manera irreversible. Para los contactos que hayan agregado el anterior número telefónico y no sean bloqueados por el usuario recibirán el nuevo número automáticamente.

### Seguridad y desarrollo

[](https://commons.wikimedia.org/wiki/File:Telegram_Chat_Secreto.PNG)

Captura del chat secreto antes de la confirmación en un iPhone.

La principal característica de Telegram es la realización de conversaciones seguras (llamado como "chats secretos"). Estas conversaciones, que se difieren a las convencionales, dejan de ser almacenadas en la nube dejando únicamente a los dispositivos del emisor y el receptor. Además, el receptor y el emisor tienen claves de cifrado distintas. Otra ventaja también relacionada con la privacidad y que se inspira de [Snapchat](https://es.wikipedia.org/wiki/Snapchat" \o "Snapchat) es la posibilidad de optar por la autodestrucción automática de los mensajes tras haber transcurrido un tiempo por determinar. Debido a la restricción a dos dispositivos bajo consentimiento y no ser compatibles con otras plataformas, los "chats secretos" son opcionales.

El 19 de diciembre de 2013 Pavel Durov anunció que daría una recompensa de US$ 200.000 en [Bitcoins](https://es.wikipedia.org/wiki/Bitcoin" \o "Bitcoin) a quien fuera capaz de romper el cifrado de la mensajería. Al finalizar el concurso un usuario descubrió un fallo relacionado con la arquitectura, obteniendo 100.000 dólares de recompensa. Este evento generó indignación en especialistas de informática debido a que el usuario "engañó" a unos cuantos mecanismos de seguridad; por lo que, según ellos, "la aplicación ofrecía una falsa sensación de privacidad".

Un año después debido a la poca expectativa de los participantes se realizó uno nuevo concurso, cuya recompensa aumentó a US$ 300.000 vía transferencia bancaria a aquel que pudiera extraer información sensible en una conversación aparentemente privada; así mismo, se añadió una bonificación independiente de US$ 100.000 en caso que se empleen [bots](https://es.wikipedia.org/wiki/Bot" \o "Bot) en lugar de usuarios.

En diciembre de 2014 se implantó en los chats secretos la tecnología Perfect forward secrecy para renovar las claves a medida que pase el tiempo sin comprometer a los mensajes antiguos.

En enero de 2015 el investigador Juliano Rizzo reveló que se empleaba en los "chats secretos" un firma digital con cifrado XOR de 128 bits usando el algoritmo SHA-1. La función del SHA-1 es codificar los mensajes con una capacidad máxima de 64 bits la mitad del cifrado XOR que se reparte tanto para el emisor y el receptor, lo que podría ser vulnerable al interferir y suplantar grandes paquetes de datos en las conversaciones. Debido a las exigencias, los desarrolladores anunciaron que el algoritmo será reemplazado por su sucesor SHA-2, incluyendo autentificaciones alternativas al SMS en caso que la clave sea descubierta.

### Móviles

* Oficiales:
  + iOS: Lanzada en agosto de 2013 para iPhone y iPod Touch y relanzado en julio de 2014 con soporte para iPad (véase *HD*), está optimizado para equipos desde la versión 6.
  + Android: Disponible desde Android 2.2, incluyendo [tablets](https://es.wikipedia.org/wiki/Tablet" \o "Tablet), cuyo mecanismo es similar. La incorporación en idioma español fue anunciada oficialmente en la versión 1.3.17.
  + Windows Phone: Basada en la aplicación Ngram, en mayo de 2014 se publicó una nueva actualización oficial en fase beta. Con una interfaz *Metro* mucho más amable para la versión 7 y superior, se han adaptado las mismas características de sus antecesores.
  + Firefox OS: Tiene un cliente oficial, disponible en Marketplace basado en Webogram con una calificación de 3+ según IARC.
  + Ubuntu Touch: Viene incluido de forma gratuita en algunos modelos.
* Ediciones comunitarias:
  + [Maemo](https://es.wikipedia.org/wiki/Maemo): Se logró adaptar la aplicación para ser utilizada en Nokia N900, hecha por usuarios de un foro.
  + Android: Previo a la decisión oficial del staff, hubo un concurso para escoger que variante usar en Telegram. El 7 de septiembrede 2013 se escogieron dos: la *N edition* de Nikolai Durov y la *S edition* de Korshakov Stepan, siendo la primera la ganadora por elección de la comunidad.
  + Blackberry OS 10: Existe una aplicación experimental, no nativa, desarrollada por Sebastian Bayerl y basada en Android. Tras un concurso para adaptar la versión nativa a mediados de 2014, donde no hubo un ganador de por medio, se hicieron seis menciones aún por pulirse. Se espera emplear un cliente ya desarrollado en mayo de 2015.
  + iOS: Telegram *HD* fue publicada en simultáneo a mediados de 2014 debido a las decisiones de organización impuestas por Apple. La diferencia es ofrecer una versión completa nativa en iPads con pantalla Retina en lugar de redimensionarlas. Esto generó críticas con la edición tradicional, confundiendo la política de revisión, por lo que fue retirada tiempo después para centrarse en una única.

**Estudio**

El estudio se realizara sobre las encuestas realizadas, de donde se obtendrán los datos necesarios para cumplir los objetivos las encuestas están basadas en un programa que utilizamos

**Objetivos**

Nuestro objetivo es analizar detalladamente la información y plasmar la importancia de esta aplicación, ya que desde la comodidad de la palma de la mano podemos organizar eventos, compartir apuntes y contenidos multimedia.

**Variables de estudio**

* Edad
* Sexo
* Ocupación
* Mesajes diarios
* Cantidad de amigos

**Relación**

No nos ha dado como resultado un buen modelo ya que los valores no se alinean.