



## Aviso de privacidad sobre los Productos y Servicios de Norton - *Actualizado por última vez el 29 de abril de 2019*

El presente Aviso ha de leerse y se aplica junto con, y como complemento a, el Aviso de privacidad global de Symantec - Norton. Describe las categorías de datos recogidos por los Productos y Servicios de Norton, así como los fines para los que se tratan esas categorías de datos. Está diseñado para ofrecer información obligatoria sobre transparencia tanto a los usuarios de Norton individuales, en calidad de interesados, y a las pymes usuarias de Norton en calidad de responsables del tratamiento de datos. Tenga en cuenta que las categorías de datos marcadas con un asterisco (\*) son datos personales transmitidos a Symantec con el fin de proporcionar las correspondientes características de productos y funcionalidades de servicios de Norton. Las restantes categorías de datos con recogidas por el software Norton de forma no identificable.

Todos los Productos y Servicios de Norton se atienen a los altos estándares establecidos en el [Aviso de privacidad global de Symantec - Norton](#). Además, para informarle de forma transparente sobre las características únicas y finalidades específicas de cada Producto y Servicio de Norton, aparte de una descripción del Producto o Servicio, el presente Aviso describe los Datos Personales que recogemos y las finalidades para las que se tratan los Datos Personales.

Si cualquier parte o aspecto de este Aviso no le resulta aceptable, le rogamos que no descargue, instale ni utilice de otra forma los correspondientes Productos, Servicios o sus funciones, o bien que desinstale o deje de utilizar inmediatamente cualquier el Producto, Servicio o funciones pertinentes. En el caso de aquellas funciones de Productos y Servicios que requieran que usted nos proporcione Datos Personales adicionales, o que requieran que usted dé su consentimiento para el tratamiento de dichos Datos Personales según sea necesario para beneficiarse de funciones opcionales específicas de un Producto o Servicio, en el momento de la descarga, instalación, activación o utilización de dicha función, se le pedirá revisar el presente Aviso para que usted pueda dar su consentimiento informado y explícito como proceda.

### Contents

Norton App Lock .....	2
Norton Clean .....	2
Norton Error Management .....	2
Norton Community Watch.....	3
Norton Core .....	4
Norton Mobile Security.....	6
Norton Security Scan.....	8
Norton Secure Login .....	9
Norton Ultimate Help-Desk y Norton Computer Tune-Up .....	10
Norton Secure VPN (previamente Norton WiFi Privacy) .....	11
Productos Norton Security (Security, Internet Security, One, Antivirus y 360).....	12
Norton Safe Search, Norton Home Page, Norton Safe Web.....	13
Norton Security Toolbar.....	15
Norton Password Manager (previamente Norton Identity Safe) .....	17
Norton Family Premier.....	18

## Norton App Lock

Descripción del Producto/Servicio	Acceso a datos y recogida	Tratamiento de datos
Norton App Lock permite al usuario proteger y mantener seguras las aplicaciones móviles utilizando un pin, contraseña o patrón para bloquearlas. En caso de que el dispositivo móvil se pierda o sea robado, App Lock también puede configurarse para que la cámara delantera del dispositivo, si está equipado con ella, tome una fotografía tras tres intentos fallidos de desbloquear el dispositivo.	<ul style="list-style-type: none"> <li>*1. Dirección de correo electrónico del usuario</li> <li>2. Configuración del usuario relativa a PIN o contraseñas de aplicaciones móviles</li> <li>3. A opción del usuario, fotos basadas en los ajustes</li> </ul>	<ul style="list-style-type: none"> <li>1. La dirección de correo electrónico del usuario se recoge y transmite a Symantec para permitir el procesamiento de las recuperaciones de contraseña y restablecimientos de Norton App Lock.</li> <li>2. 3. El resto de datos que el producto recoge de aquello que introduce el usuario se almacena en el dispositivo del usuario.</li> </ul>

## Norton Clean

Descripción del Producto/Servicio	Acceso a datos y recogida	Tratamiento de datos
Norton Clean es un optimizador de almacenamiento, que barre la memoria caché del dispositivo móvil del usuario para eliminar la publicidad y los datos no deseados liberando espacio de almacenamiento adicional.	Identificador único de dispositivo (IMEI) del dispositivo móvil	El número IMEI se recoge del dispositivo y se transmite a Symantec. Tras la transmisión al número IMEI se le aplica hash inmediatamente antes de realizar cualquier tratamiento adicional. El hash se trata con la finalidad de supervisar el uso único del producto. Una vez se ha aplicado el hash a los datos estos no pueden volver a asociarse con el dispositivo original, para que así ni el usuario ni el propio dispositivo sean rastreados ni monitorizados.

## Norton Error Management

Descripción del Producto/Servicio	Acceso a datos y recogida	Tratamiento de datos
Norton Error Management documenta los problemas que se encuentran con los productos de Norton. En estos casos el usuario puede optar por informar de los errores a Symantec.	<ul style="list-style-type: none"> <li>1. Información de estado del equipo (idioma del sistema, país y versión del sistema operativo)</li> <li>2. Procesos que se están ejecutando, su estado e información de rendimiento</li> <li>3. Datos de archivos y carpetas abiertos en el momento en que el producto de Norton encontró el problema</li> </ul>	<ul style="list-style-type: none"> <li>1.-2.-3. Symantec trata la información del sistema con la finalidad de corregir el problema encontrado y mejorar el rendimiento del producto de Norton.</li> <li>En algunos casos, si se encuentra un error debido a una amenaza o vulnerabilidad de seguridad, Symantec puede obtener y compartir ciertos datos, que no sean específicos de un usuario ni identificativos, con socios de la comunidad de ciberseguridad en general como organizaciones de investigación y otros proveedores de software de seguridad. La finalidad de compartir estos datos es la concienciación, detección y prevención de riesgos. Symantec también puede utilizar estadísticas derivadas de dicha información para realizar un seguimiento y publicar informes sobre tendencias de riesgos de seguridad.</li> </ul>

## Norton Community Watch

Descripción del Producto/Servicio	Acceso a datos y recogida	Tratamiento de datos
<p>Norton Community Watch permite a los usuarios de los productos de seguridad de Norton ayudar a mejorar la identificación y reducir el tiempo de respuesta de protección ante nuevas amenazas de seguridad. El programa recoge datos de seguridad y aplicación específicos y remite los datos a Symantec para su análisis con la finalidad de identificar nuevas amenazas y sus orígenes. El programa ayuda a construir productos de seguridad mejores y más potentes mediante el análisis de los datos enviados desde el usuario.</p> <p>Quando se une al programa Norton Community Watch:</p> <ol style="list-style-type: none"> <li>Usted participa en la construcción de una protección y de un conocimiento mejores y más sólidos frente a las ciberamenazas mediante los datos que remiten usted y otros participantes. Nuestra tecnología backend utiliza algoritmos sofisticados para calcular una calificación de reputación de seguridad para cada archivo descargado, instalado o ejecutado en su equipo, pero sin establecer nada que pudiera afectarle a usted o a cualquier tercero personalmente. Los usuarios de productos de seguridad de Norton reciben los beneficios de esta nueva tecnología innovadora cuando un producto de Norton:             <ul style="list-style-type: none"> <li>*a. Bloquea descargas dañinas mediante Download Insight. Norton le informa sobre si su descarga tiene una reputación segura o insegura o si presenta un perfil de seguridad desconocido. Si la descarga no es segura, nuestros productos actúan de forma inmediata para protegerle;</li> <li>b. Arroja unos mejores índices de detección y reduce falsos positivos;</li> <li>*c. Ejecuta escáneres más rápidos utilizando Norton Insight mediante una comprobación más veloz de archivos remitidos, analizados y declarados de buena reputación a través de Norton Community Watch.</li> </ul> </li> <li>Al proporcionar datos críticos sobre seguridad y aplicaciones usted contribuye a la inteligencia necesaria para identificar nuevas amenazas y bloquearlas antes de que se extiendan más.</li> </ol> <p>*Norton Insight solo está disponible en el sistema operativo Windows.</p>	<ol style="list-style-type: none"> <li>Identificador de equipo (datos generados por Symantec)</li> <li>Número de serie de producto (datos asignados a su producto por Symantec)</li> <li>Número de cuenta de Norton (datos generados por Symantec)</li> <li>*Rutas de archivo</li> <li>*Archivos no ejecutables y ejecutables portables identificados como malware</li> <li>URL de sitios web visitados que el producto de Norton considere potencialmente fraudulentos</li> <li>La URL del último sitio web que el usuario visitó antes de la instalación en su equipo de un riesgo de seguridad descargado</li> <li>Información sobre procesos y aplicaciones ejecutándose en el dispositivo del usuario en cualquier momento, incluyendo el momento en el que se encuentre un riesgo de seguridad potencial</li> <li>Una muestra de los datos enviados por el dispositivo del usuario en respuesta a un riesgo de seguridad potencial</li> </ol>	<p>Al tratarse Norton Community Watch de un servicio alojado y gestionado por Symantec como back-end, todos los datos recogidos se transmiten a Symantec como sigue:</p> <ol style="list-style-type: none"> <li>El identificador de equipo es necesario para realizar un seguimiento del número de dispositivos únicos que utilizan un producto por cada suscripción, para controlar y aplicar los derechos de licencia.</li> <li>El número de serie de producto se proporciona a cada usuario y se utiliza para asegurar que cada producto cuente con la licencia de uso de Symantec.</li> <li>El número de cuenta de Norton es necesario para realizar un seguimiento del número de usuarios que se suscriben a productos de Norton específicos.</li> <li>-5. Las rutas de archivo y los archivos no ejecutables y ejecutables portables se recogen para facilitar la identificación del origen y ubicación lógica de las ciberamenazas que afecten a o surjan del dispositivo del usuario.</li> <li>-7. Las URL se utilizan para identificar los orígenes en la web de riesgos de seguridad potenciales y mejorar la capacidad de los productos y servicios de Symantec para detectar acciones maliciosas, acontecimientos dañinos, sitios web fraudulentos, crimeware y otras formas de amenazas de seguridad en Internet.</li> <li>-9. Los datos de dispositivo se utilizan para mejorar los conocimientos y comprensión de Symantec respecto a las ciberamenazas. Los datos de dispositivo también se tratan para proporcionar una mejor protección a los usuarios de los productos y servicios de Symantec en el futuro y para análisis estadístico de tendencias de ciberseguridad.</li> </ol>

## Norton Core

Descripción del Producto/Servicio	Acceso a datos y recogida	Tratamiento de datos
<p>Norton Core es un router inalámbrico que proporciona protección contra malware, virus, hackers y otras ciberamenazas a los dispositivos conectados al router.</p>	<p>*1. SSID/contraseña de red inalámbrica (cifrado)</p> <p>2. Información de dispositivo, incluido cualquier dato personal introducido por el usuario al asignar nombres de dispositivo y, si lo proporciona el usuario, el nombre o seudónimo de la persona a la que está asignado el dispositivo, así como datos de agente de usuario de dispositivo/aplicaciones incluido el tipo de dispositivo, fabricante y modelo, sistema operativo y dirección IP</p> <p>3. Datos relativos al uso del dispositivo, incluidos datos sobre la hora del último uso del dispositivo, tiempo de uso de Internet para cada dispositivo conectado y registros de puerta de enlace de conexiones de red</p> <p>4. Información y configuración de control parental tal y como haya sido definido y configurado por el usuario, incluidos sitios web bloqueados, sitios web visitados e información de hora y filtro de contenidos, así como las URL de los sitios web considerados peligrosos</p> <p>*5. Datos personales que el usuario pueda proporcionar para crear una cuenta de Norton, incluido el nombre de usuario y una fotografía opcional</p> <p>*6. Datos personales proporcionados por el usuario con fines de atención al cliente y asistencia a la conectividad tales como identificador de usuario, nombre, permisos, políticas específicas de usuario e información del dispositivo</p> <p>7. Telemetría sobre ciberamenazas incluidos registros de intentos de descarga de aplicaciones móviles o archivos ejecutables maliciosos, registros de otros acontecimientos o acciones de riesgo y artefactos como muestras de malware</p> <p>*8. Información de contacto de usuario, preferencias comunicadas</p> <p>9. Dirección de envío e información relacionada</p> <p>10. Norton Core permite la participación en Norton Community Watch</p>	<p>1. La información de red inalámbrica se trata para la configuración definida por el usuario de la red wifi.</p> <p>2. La información de dispositivo se trata para la gestión de licencia, para analizar el dispositivo y su tráfico con la finalidad de supervisar la salud y conectividad del router y asistir en la resolución de problemas y para comprender el uso del dispositivo y responder ante alertas.</p> <p>3. Los datos de uso del dispositivo se tratan con las finalidades de:</p> <ul style="list-style-type: none"> <li>• Optimizar el rendimiento de Norton Core;</li> <li>• Informar a los usuarios sobre la seguridad de los sitios; y</li> <li>• Bloquear la navegación hacia sitios web no seguros.</li> </ul> <p>4. La información y configuración de control parental se utiliza para aplicar las normas y políticas definidas por el usuario para sus perfiles controlados, ayudar al usuario a detectar el uso indebido de datos personales asociados con dichos perfiles y comunicarse con el usuario y los perfiles controlados.</p> <p>5.-6. Symantec recoge la información de cuenta de usuario para prestar los servicios descritos en el contrato con el cliente y proporcionar asistencia técnica.</p> <p>7. La telemetría sobre ciberamenazas se transmite a Symantec con fines de investigación y desarrollo para mejorar los productos y servicios de Symantec y proteger mejor la red, dispositivos, datos e identidad del usuario.</p> <p>8. La información de contacto y preferencias del usuario se transmiten a Symantec con las finalidades de:</p> <ul style="list-style-type: none"> <li>• Guiar al usuario durante el proceso de instalación de software de Norton Core;</li> <li>• Informar al usuario de cómo mejorar la experiencia de usuario;</li> <li>• Adaptar la información presentada al usuario según las preferencias del usuario (como idioma o ubicación geográfica); y</li> <li>• Mejorar la satisfacción del cliente respecto a los servicios prestados mediante centros de asistencia propios y de terceros.</li> </ul> <p>9. La dirección de envío e información relacionada se trata para entregar el hardware de Norton Core al usuario.</p> <p>10. Consulte el apartado de Norton Community Watch del presente Aviso para obtener datos adicionales sobre la información relacionada con Norton Community Watch.</p> <p>Symantec utilizará además datos agregados, despersonalizados, anonimizados o no</p>

		<p>identificativos derivados de los datos recogidos, como las estadísticas, con las finalidades de:</p> <ul style="list-style-type: none"><li>• Desarrollar investigaciones generales sobre ciberseguridad;</li><li>• Mejorar la detección de malware y ciberamenazas, por ejemplo a través del análisis de muestras de archivos;</li><li>• Realizar el seguimiento y publicación de informes sobre riesgos o tendencias de seguridad y robo de identidad;</li><li>• Realizar análisis estadísticos sobre implementación de productos, incluyendo el análisis de tendencias y comparativas en nuestra base de usuarios agregada;</li><li>• Supervisión y mejora del rendimiento de los productos en lo que respecta a la disponibilidad y tiempos de respuesta;</li><li>• Conocer la frecuencia de comunicaciones relacionadas con el producto para optimizar la experiencia de usuario general; y</li><li>• Adquirir otra información comercial y de mercado no específica del usuario que sea relevante para mejorar el rendimiento de nuestra actividad.</li></ul>
--	--	---

## Norton Mobile Security

Descripción del Producto/Servicio	Acceso a datos y recogida	Tratamiento de datos
<p>Norton Mobile Security proporciona protección para smartphones y tabletas ante amenazas digitales, recuperación de dispositivos perdidos o robados e información de contacto para restauración a los usuarios protegidos y los dispositivos que el suscriptor elija proteger</p>	<ol style="list-style-type: none"> <li>1. Los datos del dispositivo móvil de usuarios protegidos, incluidos identificadores de equipo (IMEI, dirección MAC wifi, UDID, etc.), información del suscriptor, número de teléfono móvil y otra información de contacto del usuario protegido, nombre/tipo de dispositivo y fabricante, tipo y versión del sistema operativo, operador móvil, tipo de red, país de origen, identificador de caso de asistencia, certificados instalados por el usuario, nombre de dominio de sitio web y cadena de certificados SSL asociados del dispositivo y dirección IP</li> <li>2. Datos de uso como la información de descarga y frecuencia de uso, datos de registro y cookies, así como información de servicio de red sobre cómo se conecta el usuario a los servicios de red</li> <li>3. Nombres de archivos y aplicaciones en el dispositivo del usuario cada vez que el producto realice un escaneo, incluidas las aplicaciones escaneadas que no están actualmente en la base de datos de aplicaciones conocidas de Symantec para proteger al usuario ante malware o características sospechosas, así como los contenidos del calendario y las tarjetas SD si están disponibles</li> <li>4. Las URL, el historial y los marcadores de navegación</li> <li>*5. A elección del usuario, contactos en el dispositivo del usuario, incluidos registros de llamadas y SMS</li> <li>6. Configuración de audio de llamadas y del dispositivo</li> <li>*7. Datos de localización del dispositivo</li> <li>*8. El producto también puede configurarse para que, cuando se comunique que el dispositivo se ha perdido o ha sido sustraído y si este cuenta con una cámara delantera, esta tome una fotografía si el dispositivo continúa siendo utilizado, cuando se introduzca una contraseña incorrecta tras un intento fallido de desbloquear el dispositivo o si el dispositivo se</li> </ol>	<ol style="list-style-type: none"> <li>1. Los datos del dispositivo móvil, la información del suscriptor y la información de contacto del usuario protegido se tratan con las finalidades de: <ul style="list-style-type: none"> <li>• Habilitar y optimizar el funcionamiento del producto;</li> <li>• Autenticar la identidad del usuario protegido para Symantec;</li> <li>• Guiar al usuario durante el proceso de instalación de software;</li> <li>• Comunicarse con el usuario protegido para prestar el servicio;</li> <li>• Administrar la licencia; y</li> <li>• Mejorar la satisfacción del cliente respecto a los servicios prestados mediante centros de asistencia propios y de terceros.</li> </ul> </li> <li>2. Los datos de uso se tratan con las finalidades de: Conocer el uso y preferencias del producto para personalizar y mejorar la experiencia de usuario.</li> <li>3. Los archivos, nombres de aplicación, contenidos del calendario (p. ej., las URL en invitaciones) y tarjetas SD se tratan con las finalidades de: <ul style="list-style-type: none"> <li>• Alertar al usuario de aplicaciones potencialmente dañinas;</li> <li>• Escanear el dispositivo en busca de malware; y</li> <li>• Borrar contenidos personales del dispositivo si el usuario elige habilitar y ejecutar el comando Wipe del producto.</li> </ul> </li> <li>4. Los datos de navegación se tratan con las finalidades de: <ul style="list-style-type: none"> <li>• Informar a los usuarios sobre la seguridad de los sitios;</li> <li>• Bloquear la navegación hacia sitios web no seguros; y</li> <li>• Borrar el historial y marcadores de navegación si el usuario elige utilizar la característica de protección web o el comando Wipe del producto.</li> </ul> </li> <li>5. Los contactos, incluidos los registros de llamadas y SMS del dispositivo del usuario, se tratan con la finalidad de proporcionar las</li> </ol>

	<p>enciende tras haberlo apagado</p> <p>9. Copia de seguridad de los datos almacenados en el dispositivo móvil incluidos contactos, historial de llamadas, mensajes de texto y teléfonos</p>	<p>funciones de bloqueo de llamadas o SMS si el usuario elige utilizarlas.</p> <p>6. La configuración del teléfono se utiliza para bloquear llamadas entrantes de contactos o para modificar la configuración de audio del dispositivo si el usuario opta por habilitar y utilizar la característica de bloqueo o el comando Scream del producto.</p> <p>7. 8. Se pueden recoger datos de ubicación e imagen del dispositivo si lo solicita el usuario protegido para localizar el dispositivo del usuario cuando el dispositivo resulte perdido o robado. El producto también puede proporcionar al suscriptor comandos remotos para facilitar la localización del dispositivo del usuario protegido si se ha perdido o ha sido robado. En ciertos casos, cuando se comunique que el dispositivo se ha perdido o ha sido robado, el dispositivo se bloqueará de forma remota. De forma alternativa, cuando se comunique que el dispositivo se ha perdido o ha sido robado, el producto también puede cerrarse en cualquier momento. Con la autorización del usuario protegido, se podrá almacenar un historial que contenga hasta las diez últimas ubicaciones del dispositivo para permitir al usuario protegido rastrear los movimientos recientes del dispositivo, incluso si no se está utilizando el producto en ese momento.</p> <p>9. Los datos de copia de seguridad se tratan con la finalidad de proporcionar las características de copia de seguridad y recuperación del producto si el usuario elige utilizarlas.</p> <p>Symantec utilizará además datos agregados, despersonalizados, anonimizados o no identificativos derivados de los datos recogidos, como las estadísticas, con las finalidades de:</p> <ul style="list-style-type: none"><li>• Desarrollar investigaciones generales sobre ciberseguridad;</li><li>• Mejorar la detección de malware y ciberamenazas, por ejemplo a través del análisis de muestras de archivos;</li><li>• Realizar el seguimiento y publicación de informes sobre riesgos o tendencias de seguridad y robo de identidad;</li><li>• Realizar análisis estadísticos sobre implementación de productos, incluyendo el análisis de tendencias y comparativas en nuestra base de usuarios agregada;</li><li>• Supervisión y mejora del rendimiento de los productos en lo que respecta a la disponibilidad y tiempos de respuesta;</li><li>• Conocer la frecuencia de comunicaciones relacionadas con el producto para optimizar la experiencia de usuario general; y</li><li>• Adquirir otra información comercial y de mercado no específica del usuario que sea relevante para mejorar el rendimiento de nuestra actividad.</li></ul>
--	--	---

Descripción del Producto/Servicio	Acceso a datos y recogida	Tratamiento de datos
<p>Norton Secure Scan escanea los dispositivos finales seleccionados por el usuario para identificar riesgos y problemas potenciales y recomienda productos y soluciones al usuario.</p>	<p>1. Identificadores de equipo (datos generados internamente por Symantec); función de instalación/desinstalación del dispositivo; información de dispositivo y datos de agente de usuario del dispositivo/aplicación incluido el tipo de dispositivo, versión e idioma del sistema operativo, fabricante y modelo; sistema operativo e información geográfica asociada</p> <p>2. Información de telemetría sobre archivos escaneados, la experiencia de usuario y las amenazas encontradas, solucionadas y existentes; fecha y hora del escáner tras el envío; información de estado relativa a la instalación y operación, que puede incluir incidentalmente datos personales si se encuentran en una ruta de archivo o nombre de carpeta</p>	<p>1. Symantec utiliza los identificadores de equipo y la información relacionada con las finalidades de:</p> <ul style="list-style-type: none"> <li>• Guiar al usuario durante el proceso de instalación de software;</li> <li>• Comunicarse con el usuario para prestar el servicio;</li> <li>• Conocer el uso y preferencias del servicio para personalizar y mejorar la experiencia de usuario.</li> </ul> <p>2. Symantec utiliza la información de telemetría con las finalidades de:</p> <ul style="list-style-type: none"> <li>• Habilitar y optimizar el funcionamiento del servicio; y</li> <li>• Con fines de investigación y desarrollo para mejorar los productos y servicios de Symantec y proteger mejor la red, dispositivos, datos e identidad del usuario.</li> </ul> <p>Symantec utilizará además datos agregados, despersonalizados, anonimizados o no identificativos derivados de los datos recogidos, como las estadísticas, con las finalidades de:</p> <ul style="list-style-type: none"> <li>• Desarrollar investigaciones generales sobre ciberseguridad;</li> <li>• Mejorar la detección de malware y ciberamenazas, por ejemplo a través del análisis de muestras de archivos;</li> <li>• Realizar el seguimiento y publicación de informes sobre riesgos o tendencias de seguridad y robo de identidad;</li> <li>• Realizar análisis estadísticos sobre implementación de productos, incluyendo el análisis de tendencias y comparativas en nuestra base de usuarios agregada;</li> <li>• Supervisión y mejora del rendimiento de los productos en lo que respecta a la disponibilidad y tiempos de respuesta;</li> <li>• Conocer la frecuencia de comunicaciones relacionadas con el producto para optimizar la experiencia de usuario general; y</li> <li>• Adquirir otra información comercial y de mercado no específica del usuario que sea relevante para mejorar el rendimiento de nuestra actividad.</li> </ul>



## Norton Secure Login

Descripción del Producto/Servicio	Acceso a datos y recogida	Tratamiento de datos
<p>Norton Secure Login (NSL) es un Proveedor de Identidad que ofrece una forma sencilla, segura y centralizada de autenticar a los usuarios. Symantec ofrece una infraestructura para la gestión de la identidad a millones de usuarios en varios productos de Norton.</p>	<p>*1. Datos personales para facilitar la autenticación de la identidad del usuario tales como dirección, número de teléfono, fecha de nacimiento o tarjeta de crédito; información de contacto del usuario; cualesquiera datos personales que el usuario introduzca en la cuenta de Norton del usuario o que el usuario pueda proporcionar con fines de atención al cliente y ayuda a la conectividad tales como el nombre e información del dispositivo</p> <p>2. Información del dispositivo, del producto y del servicio y datos de agente de usuario del dispositivo/aplicación incluido el tipo de dispositivo; fabricante; modelo; sistema operativo y versión; información del dispositivo y datos de agente de usuario del dispositivo/aplicación incluido el tipo de dispositivo; fabricante; modelo; sistema operativo y versión; datos sobre rendimiento de tiempo de ejecución; aplicaciones instaladas; información geográfica asociada, dirección MAC y dirección IP</p> <p>3. Datos de uso relativos al uso de Internet tales como las URL y direcciones IP de sitios web visitados, palabras y resultados de búsqueda e información sobre riesgos de seguridad potenciales (incluidas URL y direcciones IP de sitios web considerados potencialmente fraudulentos, que pueden contener datos personales que el sitio web intente obtener sin la autorización del usuario)</p>	<p>1. Symantec trata los datos personales con las finalidades de:</p> <ul style="list-style-type: none"> <li>• Autenticar la identidad del usuario para Symantec o establecer la fiabilidad de terceros que utilicen Norton Security Login;</li> <li>• Emitir credenciales de identidad o evitar transacciones fraudulentas en nombre del usuario;</li> <li>• Guiar al usuario durante el proceso de instalación;</li> <li>• Comunicarse con el usuario para prestar servicios como ayuda o asistencia; y</li> <li>• Mejorar la satisfacción del cliente respecto a los servicios prestados mediante centros de asistencia propios y de terceros.</li> </ul> <p>2. Symantec trata la información del dispositivo, del producto y del servicio con las finalidades de:</p> <ul style="list-style-type: none"> <li>• Habilitar y optimizar el funcionamiento de los productos y servicios;</li> <li>• Administrar la licencia; y</li> <li>• Conocer el uso y preferencias del producto para personalizar y mejorar la experiencia de usuario.</li> </ul> <p>3. Symantec trata los datos de uso con las finalidades de:</p> <ul style="list-style-type: none"> <li>• Informar a los usuarios sobre la seguridad de los sitios;</li> <li>• Bloquear la navegación hacia sitios web no seguros; y</li> <li>• Con fines de investigación y desarrollo para mejorar los productos y servicios de Symantec y proteger mejor la red, dispositivos, datos e identidad del usuario.</li> </ul> <p>Symantec utilizará además datos agregados, despersonalizados, anonimizados o no identificativos derivados de los datos recogidos, como las estadísticas, con las finalidades de:</p> <ul style="list-style-type: none"> <li>• Desarrollar investigaciones generales sobre ciberseguridad;</li> <li>• Mejorar la detección de malware y ciberamenazas, por ejemplo a través del análisis de muestras de archivos;</li> <li>• Realizar el seguimiento y publicación de informes sobre riesgos o tendencias de seguridad y robo de identidad;</li> <li>• Realizar análisis estadísticos sobre implementación de productos, incluyendo el análisis de tendencias y comparativas en nuestra base de usuarios agregada;</li> <li>• Supervisión y mejora del rendimiento de los productos en lo que respecta a la disponibilidad y tiempos de respuesta;</li> <li>• Conocer la frecuencia de comunicaciones relacionadas con el producto para optimizar la experiencia de usuario general; y</li> <li>• Adquirir otra información comercial y de mercado no específica del usuario que sea relevante para mejorar el rendimiento de nuestra actividad.</li> </ul>

## Norton Ultimate Help-Desk y Norton Computer Tune-Up

Descripción del Producto/Servicio	Acceso a datos y recogida	Tratamiento de datos
<p>Norton Ultimate Help Desk permite al usuario contactar con un experto para recibir asistencia con cuestiones técnicas que pueden ir desde la configuración de la red hasta el diagnóstico del dispositivo y resolución de problemas.</p> <p>Norton Computer Tune-Up es una característica incluida en Norton Ultimate Help Desk que facilita que el dispositivo del usuario siga funcionando como nuevo utilizando el diagnóstico.</p>	<p>*1. La información de solicitud que usted proporcione a los representantes del servicio de atención de Symantec por teléfono o que introduzca en la interfaz en línea de Symantec cuando solicite los servicios de Norton</p> <p>2. Información del sistema incluido: Tipo y versión del sistema operativo y navegador utilizados en su dispositivo; si existe un firewall activo; si hay instalado software antivirus y si se está ejecutando y está actualizado; espacio en memoria y en disco, configuración de proxy y listados de directorios para la herramienta de asistencia de software; información del navegador incluida la configuración de seguridad y archivos temporales; puertos activos, archivo hosts y configuración de interfaz de red del dispositivo; programas instalados e información de procesos activos; archivo de registro de aplicación y sistema operativo y datos de registro</p> <p>3. Información de diagnóstico incluido: Número de archivos escaneados, amenazas detectadas y amenazas solucionadas por la herramienta de asistencia de software; tipos de amenazas encontradas; el estado de seguridad (bueno/normal/malo) del dispositivo según determine la herramienta de asistencia de software; número y tipo de amenazas restantes que la herramienta de asistencia de software no haya podido solucionar</p>	<p>1. Symantec trata la información de solicitud con las finalidades de:</p> <ul style="list-style-type: none"> <li>• Comunicarse con el usuario para prestar el servicio;</li> <li>• Conocer el uso y preferencias del producto para personalizar y mejorar la experiencia de usuario; y</li> <li>• Mejorar la satisfacción del cliente respecto a los servicios prestados mediante centros de asistencia propios y de terceros.</li> </ul> <p>2. Symantec trata la información de sistema con las finalidades de:</p> <ul style="list-style-type: none"> <li>• Prestar los servicios solicitados por el usuario;</li> <li>• Habilitar y optimizar el funcionamiento de los servicios; y</li> <li>• Guiar al usuario durante la utilización de los servicios.</li> </ul> <p>3. Symantec trata la información de diagnóstico con las finalidades de:</p> <ul style="list-style-type: none"> <li>• Informar al usuario del resultado de los servicios prestados; y</li> <li>• Con fines de investigación y desarrollo para mejorar los productos y servicios de Symantec y proteger mejor la red, dispositivos, datos e identidad del usuario.</li> </ul> <p>Syantec utilizará además datos agregados, despersonalizados, anonimizados o no identificativos derivados de los datos recogidos, como las estadísticas, con las finalidades de:</p> <ul style="list-style-type: none"> <li>• Desarrollar investigaciones generales sobre ciberseguridad;</li> <li>• Mejorar la detección de malware y ciberamenazas, por ejemplo a través del análisis de muestras de archivos;</li> <li>• Realizar el seguimiento y publicación de informes sobre riesgos o tendencias de seguridad y robo de identidad;</li> <li>• Realizar análisis estadísticos sobre implementación de productos, incluyendo el análisis de tendencias y comparativas en nuestra base de usuarios agregada;</li> <li>• Supervisión y mejora del rendimiento de los productos en lo que respecta a la disponibilidad y tiempos de respuesta;</li> <li>• Conocer la frecuencia de comunicaciones relacionadas con el producto para optimizar la experiencia de usuario general; y</li> <li>• Adquirir otra información comercial y de mercado no específica del usuario que sea relevante para mejorar el rendimiento de nuestra actividad.</li> </ul>

## Norton Secure VPN (previamente Norton WiFi Privacy)

Descripción del Producto/Servicio	Acceso a datos y recogida	Tratamiento de datos
<p>Norton Secure VPN protege los dispositivos y datos del usuario mediante el cifrado de la información del usuario en cualquier conexión a Internet y manteniendo la privacidad del usuario.</p>	<ol style="list-style-type: none"> <li>1. Información del suscriptor y datos del dispositivo móvil incluido el nombre y tipo de dispositivo, versión del sistema operativo e idioma;</li> <li>2. Uso agregado de ancho de banda;</li> <li>3. Datos de uso temporales para asistir en la resolución de un problema con el servicio.</li> </ol>	<ol style="list-style-type: none"> <li>1. Symantec trata la información del suscriptor y los datos del dispositivo móvil con las finalidades de: <ul style="list-style-type: none"> <li>• Habilitar y optimizar el funcionamiento de los servicios;</li> <li>• Conocer el uso y preferencias del producto para personalizar y mejorar la experiencia de usuario;</li> <li>• Guiar al usuario durante la instalación del software y el uso del servicio;</li> <li>• Comunicarse con el usuario para prestar el servicio;</li> <li>• Recordar al usuario proteger la información que esté transmitiendo; y</li> <li>• Mejorar la satisfacción del cliente respecto a los servicios prestados mediante centros de asistencia propios y de terceros.</li> </ul> </li> <li>2. Symantec trata los datos de uso de ancho de banda con fines de facturación, operaciones de red y asistencia.</li> <li>3. Symantec trata los datos de uso temporales con las finalidades de: <ul style="list-style-type: none"> <li>• Elegir el servidor más adecuado al que conectarse; y</li> <li>• Con fines de investigación y desarrollo para mejorar los productos y servicios de Symantec y proteger mejor la red, dispositivos, datos e identidad del usuario.</li> </ul> </li> </ol> <p>Mientras se utiliza Norton Secure VPN el tráfico de Internet del usuario se enruta a través de la red de Symantec, que es una red "Sin registro". Esto quiere decir que Symantec no almacena la dirección IP origen del usuario cuando se conecta a Norton Secure VPN y por lo tanto Symantec no puede identificar a los individuos. La gestión del tráfico automatizada basada en reglas de Symantec puede requerir el análisis en tiempo real del tráfico de datos de Internet incluidos los sitios web o direcciones IP de destino y direcciones IP origen, aunque no se mantiene ningún registro de esta información. Symantec no almacena información sobre aplicaciones, servicios o sitios web que el usuario descargue, utilice o visite. Puesto que Symantec gestiona una red mundial, el tráfico de Internet del usuario puede enrutarse a través de uno o más países tal y como se explica en el <a href="#">Aviso de privacidad global de Symantec - Norton</a>.</p> <p>Symantec utilizará además datos agregados, despersonalizados, anonimizados o no identificativos derivados de los datos recogidos, como las estadísticas, con las finalidades de:</p> <ul style="list-style-type: none"> <li>• Desarrollar investigaciones generales sobre ciberseguridad;</li> <li>• Mejorar la detección de malware y ciberamenazas, por ejemplo a través del análisis de muestras de archivos;</li> <li>• Realizar el seguimiento y publicación de informes sobre riesgos o tendencias de seguridad y robo de identidad;</li> <li>• Realizar análisis estadísticos sobre implementación de productos, incluyendo el análisis de tendencias y comparativas en nuestra base de usuarios agregada;</li> <li>• Supervisión y mejora del rendimiento de los productos en lo que respecta a la disponibilidad y tiempos de respuesta;</li> <li>• Conocer la frecuencia de comunicaciones relacionadas con el producto para optimizar la experiencia de usuario general; y</li> <li>• Adquirir otra información comercial y de mercado no específica del usuario que sea relevante para mejorar el rendimiento de nuestra actividad.</li> </ul>

## Productos Norton Security (Security, Internet Security, One, Antivirus y 360)

Este apartado cubre Norton Security (Standard, Deluxe y Premium), Norton Internet Security, Norton One, Norton Antivirus, Norton Antivirus Basic, Norton 360, Norton 360PE y Norton 360MD.

Descripción del Producto/Servicio	Acceso a datos y recogida	Tratamiento de datos
<p>Los productos de Norton Security proporcionan seguridad a los dispositivos finales defendiéndolos ante ransomware, virus, spyware, malware y otras ciberamenazas.</p>	<p>1. Información del suscriptor y datos del dispositivo incluidos *datos personales que el usuario pueda introducir para crear una cuenta de Norton tales como el nombre de usuario y una fotografía opcional; cualquier *dato personal que el usuario incluya al asignar los nombres de dispositivo y, en caso de proporcionarse, el nombre o seudónimo de la persona a la que está asignado el dispositivo, así como datos de agente de usuario del dispositivo/aplicación incluido el tipo de dispositivo, fabricante y modelo; sistema operativo y versión; aplicaciones y versiones; información geográfica asociada, dirección MAC, identificador de equipo y direcciones IP; información de estado relativa a la instalación y operación que puede incluir datos personales de forma incidental si están en un nombre de archivo o carpeta; cualquier dato personal que el usuario proporcione a Symantec con fines de atención al cliente y ayuda a la conectividad tales como identificador de usuario, nombre, permisos, políticas e información del dispositivo</p> <p>2. Datos relativos al uso de Internet tales como las URL y direcciones IP de sitios web visitados, palabras y resultados de búsqueda e información sobre riesgos de seguridad potenciales (incluidas URL y direcciones IP de sitios web considerados potencialmente fraudulentos, que pueden contener datos personales que el sitio web intente obtener sin la autorización del usuario)</p> <p>3. Datos relacionados con el uso del dispositivo y diagnóstico, incluidos: Datos relativos a la hora del último uso del dispositivo, tiempo de uso de Internet para</p>	<p>1. Symantec trata la información del suscriptor y los datos del dispositivo con las finalidades de:</p> <ul style="list-style-type: none"> <li>• Habilitar y optimizar el funcionamiento de los productos y servicios;</li> <li>• Autenticar la identidad del usuario para Symantec;</li> <li>• Conocer el uso y preferencias del producto para personalizar y mejorar la experiencia de usuario;</li> <li>• Guiar al usuario durante el proceso de instalación de software;</li> <li>• Comunicarse con el usuario para prestar el servicio;</li> <li>• Administrar la licencia; y</li> <li>• Mejorar la satisfacción del cliente respecto a los servicios prestados mediante centros de asistencia propios y de terceros.</li> </ul> <p>2. Los datos de uso de Internet se tratan con las finalidades de:</p> <ul style="list-style-type: none"> <li>• Informar al usuario sobre la seguridad de los sitios; y</li> <li>• Bloquear la navegación hacia sitios web no seguros.</li> </ul> <p>3. Symantec trata los datos de uso del dispositivo y de diagnóstico con las finalidades de:</p> <ul style="list-style-type: none"> <li>• Conocer el uso del producto;</li> <li>• Proporcionar las características de protección de los productos y servicios; y</li> <li>• Con fines de investigación y desarrollo para mejorar los productos y servicios de Symantec y proteger mejor la red, dispositivos, datos e identidad del usuario.</li> </ul> <p>4. La información y configuración de control parental se utiliza para aplicar las normas y políticas definidas por el usuario para sus perfiles controlados, ayudar al usuario a detectar el uso indebido de datos personales asociados con dichos perfiles y comunicarse con el usuario y los perfiles controlados.</p> <p>Syantec utilizará además datos agregados, despersonalizados, anonimizados o no identificativos derivados de los datos recogidos, como las estadísticas, con las finalidades de:</p> <ul style="list-style-type: none"> <li>• Desarrollar investigaciones generales sobre ciberseguridad;</li> <li>• Mejorar la detección de malware y ciberamenazas, por ejemplo a</li> </ul>

	<p>cada dispositivo conectado y registros de puerta de enlace con información sobre las actividades de conexión de red; archivos ejecutables identificados como malware potencial, que podrían incluir datos personales obtenidos por el malware sin la autorización del usuario; mensajes de correo electrónico enviados a Symantec con la autorización del usuario clasificados como spam o identificados incorrectamente como spam; información “Crash dump” o información contenida en un informe que el usuario opte por enviar a Symantec cuando los productos y servicios encuentren un problema y que puede incluir el idioma del sistema, país, sistema operativo y procesos o archivos ejecutándose en el momento del error</p> <p>4. Información y configuración de control parental tal y como haya sido definido y configurado por el usuario, incluidos sitios web bloqueados, sitios web visitados e información de hora y filtro de contenidos, así como las URL de los sitios web considerados peligrosos.</p>	<p>través del análisis de muestras de archivos;</p> <ul style="list-style-type: none"> <li>• Realizar el seguimiento y publicación de informes sobre riesgos o tendencias de seguridad y robo de identidad;</li> <li>• Realizar análisis estadísticos sobre implementación de productos, incluyendo el análisis de tendencias y comparativas en nuestra base de usuarios agregada;</li> <li>• Supervisión y mejora del rendimiento de los productos en lo que respecta a la disponibilidad y tiempos de respuesta;</li> <li>• Conocer la frecuencia de comunicaciones relacionadas con el producto para optimizar la experiencia de usuario general; y</li> <li>• Adquirir otra información comercial y de mercado no específica del usuario que sea relevante para mejorar el rendimiento de nuestra actividad.</li> </ul>
--	---	---

## Norton Safe Search, Norton Home Page, Norton Safe Web

Descripción del Producto/Servicio	Acceso a datos y recogida	Tratamiento de datos
<p>Norton Safe Search es un sitio web de motor de búsqueda que ayuda a proteger a los usuarios de sitios web no seguros filtrando los resultados de búsqueda y proporcionando puntuaciones de seguridad de sitios web a los usuarios para proporcionar una experiencia de navegación más segura. También es una extensión para navegadores que proporciona acceso al sitio web de Norton Safe Search de varias formas. Diferentes versiones de esta extensión pueden a elección del usuario o bien:</p> <p>a) reemplazar el motor de búsqueda predeterminado del navegador por el sitio web de Norton Safe Search o bien;</p> <p>b) reemplazar el motor de búsqueda predeterminado del navegador por el sitio web de Norton Safe Search Y reemplazar la página de inicio predeterminada del navegador</p>	<ol style="list-style-type: none"> <li>1. Información del suscriptor y datos del dispositivo y de software, incluidos: Nombre del navegador, versión y preferencias de idioma; sistema operativo, versión o plataforma; dirección IP del dispositivo del usuario</li> <li>2. Datos de uso del servicio incluidos; Enlaces web en redes sociales y webmail; Actividad de navegación web; términos de búsqueda web; entradas predeterminadas en diferentes cuadros de búsqueda gestionados por los productos de Norton; resultados del motor de búsqueda</li> <li>3. Cookies, etiquetas pixel, scripts o tecnologías similares colocadas en el ordenador o dispositivo por el sitio web de Norton Safe Search y el sitio web de Norton Home Page</li> </ol>	<ol style="list-style-type: none"> <li>1. Symantec trata la información del suscriptor y los datos del dispositivo y de software con las finalidades de: <ul style="list-style-type: none"> <li>• Habilitar y optimizar el funcionamiento de los productos y servicios;</li> <li>• Administrar la licencia;</li> <li>• Conocer el uso y preferencias del producto para personalizar y mejorar la experiencia de usuario;</li> <li>• Guiar al usuario durante el proceso de instalación de software;</li> <li>• Proporcionar mejoras de los productos y servicios para proteger mejor al usuario y a la red, dispositivo,</li> </ul> </li> </ol>

<p>+ la configuración de nueva pestaña por Norton Home Page.</p> <p>Norton Home Page es una extensión de navegador y página de inicio predeterminada que habilita el sitio web de Norton Safe Search.</p> <p>Norton Safe Web es una extensión de navegador que el usuario puede elegir utilizar para supervisar la actividad de navegación y el contenido de las páginas web. Utiliza servicios de reputación y análisis de contenidos de páginas web para ayudar a proteger al usuario de contenidos de sitios web maliciosos, phishing y otras amenazas.</p>		<p>datos e identidad del usuario; y</p> <ul style="list-style-type: none"><li>• Mejorar la satisfacción del cliente respecto a los servicios prestados mediante centros de asistencia propios y de terceros.</li></ul> <p>2. Los datos de uso del servicio son tratados por Symantec y en nombre de Symantec con las finalidades de:</p> <ul style="list-style-type: none"><li>• Informar a los usuarios sobre la seguridad de los sitios;</li><li>• Bloquear la navegación hacia sitios web no seguros; y</li><li>• Analizar el uso del servicio.</li></ul> <p>Las solicitudes de búsqueda realizadas a través de nuestro producto Norton Safe Search se dirigirán a nuestros socios terceros de búsqueda Oath/Yahoo! (para los EE. UU. y Canadá) e IACI (para fuera de los EE. UU. y Canadá) para que se le proporcionen a usted los resultados de búsqueda. Nuestros socios terceros también pueden recoger información directamente de usted de acuerdo con su actividad en Norton Safe Search. Nuestros socios terceros recogerán dichos datos en calidad de responsables con la finalidad de tratar sus solicitudes de búsqueda. Dicha recogida de datos se rige por la Política, Declaración y Aviso de privacidad de los socios terceros.</p> <p>Para que pueda utilizar Norton Safe Search, sus solicitudes de búsqueda se dirigirán a nuestros socios terceros (empresas que no pertenecen a Symantec) y dichos terceros procesarán su solicitud. Los socios terceros también pueden recopilar información directamente de usted mediante su actividad en Norton Safe Search (conjuntamente, “datos de terceros”). El socio tercero será el responsable del tratamiento de los datos con la finalidad de procesar su solicitud de búsqueda, por lo que es nuestro socio tercero y no Symantec quien decide cómo se recogerán, utilizarán, revelarán, conservarán o tratarán de otro modo sus datos. Sus datos de terceros están sujetos a los avisos de privacidad del socio tercero para el tratamiento de sus datos para la realización de la búsqueda. Le rogamos que consulte los avisos de privacidad de nuestro socio <a href="#">tercero localizados</a>.</p> <p>3. Las cookies y tecnologías de rastreo similares se tratan con la finalidad de realizar un seguimiento de las preferencias e historial de uso de las características. Para obtener más información sobre cookies consulte el apartado anterior titulado “Tecnologías de seguimiento, cookies y No rastrear” del <a href="#">Aviso de privacidad global de Symantec - Norton</a>.</p> <p>El protocolo de medición de <a href="#">Google Analytics</a> trata <a href="#">Direcciones IP anonimizadas</a> e información de uso del producto con finalidades de análisis estadístico y gestión de errores</p>
--	--	--

		<p>críticos. Haga clic aquí para obtener información <a href="#">sobre la protección de datos de Google Analytics</a>.</p> <p>Symantec utilizará además datos agregados, despersonalizados, anonimizados o no identificativos derivados de los datos recogidos, como las estadísticas, con las finalidades de:</p> <ul style="list-style-type: none"> <li>• Desarrollar investigaciones generales sobre ciberseguridad;</li> <li>• Mejorar la detección de malware y ciberamenazas, por ejemplo a través del análisis de muestras de archivos;</li> <li>• Realizar el seguimiento y publicación de informes sobre riesgos o tendencias de seguridad y robo de identidad;</li> <li>• Realizar análisis estadísticos sobre implementación de productos, incluyendo el análisis de tendencias y comparativas en nuestra base de usuarios agregada; y</li> <li>• Supervisión y mejora del rendimiento de los productos en lo que respecta a la disponibilidad y tiempos de respuesta.</li> </ul>
--	--	--

## Norton Security Toolbar

Descripción del Producto/Servicio	Acceso a datos y recogida	Tratamiento de datos
<p>Norton Security Toolbar presenta dos variantes: a) un complemento de Microsoft Internet Explorer y b) una extensión de navegador para Google Chrome. El usuario puede utilizar las dos variantes para supervisar la actividad de navegación del usuario y el contenido de páginas web. Ambas emplean servicios de reputación y análisis del contenido de páginas web para ayudar a proteger al usuario de contenidos de sitios web maliciosos, phishing y otras amenazas.</p> <p>La variante de Internet Explorer permite el acceso y utilización del depósito de información de Norton Password Manager dentro de la interfaz de usuario del navegador. También proporciona un cuadro de búsqueda para realizar búsquedas en el sitio web de Norton Safe Search. La variante de Google Chrome proporciona un cuadro de búsqueda para realizar búsquedas en el sitio web de Norton Safe Search.</p>	<ol style="list-style-type: none"> <li>1. Datos de dispositivo y de software, incluidos: Nombre del navegador, versión y preferencias de idioma; sistema operativo, versión o plataforma; dirección IP del dispositivo del usuario</li> <li>2. Datos de uso del producto incluidos: Actividad de navegación web; historial de navegación web limitado; términos de búsqueda; entradas predeterminadas en diferentes cuadros de búsqueda gestionados por los productos de Norton; resultados del motor de búsqueda</li> <li>3. Cookies, etiquetas pixel, scripts o tecnologías similares colocadas en el ordenador o dispositivo por el sitio web de Norton Safe Search y el sitio web de Norton Home Page</li> </ol>	<ol style="list-style-type: none"> <li>1. Symantec trata los datos de dispositivos y software con las finalidades de: <ul style="list-style-type: none"> <li>• Habilitar y optimizar el funcionamiento de los productos y servicios;</li> <li>• Administrar la licencia;</li> <li>• Conocer el uso y preferencias del producto para personalizar y mejorar la experiencia de usuario;</li> <li>• Guiar al usuario durante el proceso de instalación de software;</li> <li>• Proporcionar mejoras de los productos y servicios para proteger mejor al usuario y a la red, dispositivo, datos e identidad del usuario; y</li> <li>• Mejorar la satisfacción del cliente respecto a los servicios</li> </ul> </li> </ol>

		<p>prestados mediante centros de asistencia propios y de terceros.</p> <p>2. Los datos de uso del producto son tratados por Symantec y en nombre de Symantec con las finalidades de:</p> <ul style="list-style-type: none"><li>• Informar a los usuarios sobre la seguridad de los sitios;</li><li>• Bloquear la navegación hacia sitios web no seguros; y</li><li>• Analizar el uso del servicio.</li></ul> <p>3. Las cookies y tecnologías de rastreo similares se tratan con la finalidad de realizar un seguimiento de las preferencias e historial de uso de las características. Para obtener más información sobre cookies consulte el apartado anterior titulado “Tecnologías de seguimiento, cookies y No rastrear” del <a href="#">Aviso de privacidad global de Symantec - Norton</a>.</p> <p>Symantec utilizará además datos agregados, despersonalizados, anonimizados o no identificativos derivados de los datos recogidos, como las estadísticas, con las finalidades de:</p> <ul style="list-style-type: none"><li>• Desarrollar investigaciones generales sobre ciberseguridad;</li><li>• Mejorar la detección de malware y ciberamenazas, por ejemplo a través del análisis de muestras de archivos;</li><li>• Realizar el seguimiento y publicación de informes sobre riesgos o tendencias de seguridad y robo de identidad;</li><li>• Realizar análisis estadísticos sobre implementación de productos, incluyendo el análisis de tendencias y comparativas en nuestra base de usuarios agregada; y</li><li>• Supervisión y mejora del rendimiento de los productos en lo que respecta a la disponibilidad y tiempos de respuesta.</li></ul>
--	--	---



## Norton Password Manager (previamente Norton Identity Safe)

Descripción del Producto/Servicio	Acceso a datos y recogida	Tratamiento de datos
<p>Norton Password Manager presenta dos variantes: a) un componente de Norton Security y b) extensiones de navegador para los principales navegadores salvo Internet Explorer. Todas las variantes consisten en un gestor de contraseñas que gestiona nombres de usuario, contraseñas y otra información útil para desarrollar actividades en línea.</p>	<p>1. Información del suscriptor y datos del dispositivo y de software, incluidos: Nombre del navegador, versión y preferencias de idioma; sistema operativo, versión o plataforma; dirección IP del dispositivo del usuario; *otros datos personales revelados por el usuario como nombres de usuario, contraseñas, direcciones de sitios web, direcciones físicas, números de cuenta de pago, información de caducidad y texto de formulario abierto</p> <p>2. Datos de uso del servicio incluidos: Actividad de navegación web; términos de búsqueda web; entradas predeterminadas en diferentes cuadros de búsqueda gestionados por los productos de Norton; resultados del motor de búsqueda</p>	<p>1. Symantec trata los datos de dispositivos y software con las finalidades de:</p> <ul style="list-style-type: none"> <li>• Habilitar y optimizar el funcionamiento de los productos y servicios;</li> <li>• Administrar la licencia;</li> <li>• Conocer el uso y preferencias del producto para personalizar y mejorar la experiencia de usuario;</li> <li>• Guiar al usuario durante el proceso de instalación de software;</li> <li>• Proporcionar mejoras de los productos y servicios para proteger mejor al usuario y a la red, dispositivo, datos e identidad del usuario; y</li> <li>• Mejorar la satisfacción del cliente respecto a los servicios prestados mediante centros de asistencia propios y de terceros.</li> </ul> <p>2. Los datos de uso del producto son tratados por Symantec y en nombre de Symantec con las finalidades de:</p> <ul style="list-style-type: none"> <li>• Informar a los usuarios sobre la seguridad de los sitios;</li> <li>• Bloquear la navegación hacia sitios web no seguros; y</li> <li>• Analizar el uso del servicio.</li> </ul> <p>El protocolo de medición de <a href="#">Google Analytics</a> trata <a href="#">Direcciones IP anonimizadas</a> e información de uso del producto con finalidades de análisis estadístico y gestión de errores críticos. Haga clic aquí para obtener información <a href="#">sobre la protección de datos de Google Analytics</a>.</p> <p>Symantec utilizará además datos agregados, despersonalizados, anonimizados o no identificativos derivados de los datos recogidos, como las estadísticas, con las finalidades de:</p> <ul style="list-style-type: none"> <li>• Desarrollar investigaciones generales sobre ciberseguridad;</li> <li>• Mejorar la detección de malware y ciberamenazas, por ejemplo a través del análisis de muestras de archivos;</li> <li>• Realizar el seguimiento y publicación de informes sobre riesgos o tendencias de seguridad y robo de identidad;</li> <li>• Realizar análisis estadísticos sobre implementación de productos, incluyendo el análisis de tendencias y comparativas en nuestra base de usuarios agregada; y</li> <li>• Supervisión y mejora del rendimiento de los productos en lo que respecta a la disponibilidad y tiempos de respuesta.</li> </ul>

## Norton Family Premier

Descripción del producto/servicio	Acceso a datos y recogida	Tratamiento de datos
<p>Norton Family Premier ayuda a proteger a los usuarios protegidos y los dispositivos que el suscriptor elija proteger con controles parentales aplicados mediante configuraciones y características de protección definidas y gestionadas por el suscriptor.</p> <p>Para obtener más información sobre Norton Family Premier consulte el apartado "Información adicional sobre Norton Family Premier" más adelante</p>	<p>*1. Información del suscriptor como: Información de contacto del administrador incluyendo, entre otros, nombre del suscriptor, dirección de correo electrónico y contraseña para proteger la cuenta del suscriptor; datos personales proporcionados por el suscriptor durante la configuración del servicio o cualquier otra llamada de asistencia posterior;</p> <p>2. Datos de dispositivo y de software, incluidos: Estado de la instalación del software cliente de Norton Family en el dispositivo del suscriptor o del usuario protegido; configuración de software, información de producto y estado de la instalación; estado de la licencia, información de derechos de licencia, identificador de licencia y uso de la licencia; nombre del dispositivo, tipo, versión del sistema operativo, idioma, ubicación (Sistema de Posicionamiento Global, GPS), tipo y versión del navegador; hardware, software e inventario de aplicaciones del dispositivo; configuraciones de acceso, requisitos de política y estado de cumplimiento de la política de aplicaciones y base de datos, así como registros de excepciones y errores de flujo de trabajo de aplicaciones;</p> <p>*3. Información del usuario protegido que el suscriptor opte por revelar a Symantec, incluido: Nombre, sexo, edad y año de nacimiento; imágenes de avatar; los últimos seis dígitos de números de identificación oficiales relacionados con el usuario protegido (p. ej., cuando existan: número de la Seguridad Social, número de identificación nacional, etc.), dirección de correo electrónico, número de teléfono móvil, nombre de la institución educativa o cualquier otra información que el suscriptor desee proteger; información de inicio de sesión en el equipo, país y zona horaria;</p> <p>4. Información de actividad red del usuario protegido que el suscriptor solicite a Symantec supervisar, lo que incluye a plena discreción del suscriptor: Actividades y ubicaciones en línea y de dispositivos móviles; sitios web que el usuario protegido intente visitar y aquellos que el producto</p>	<p>1. Symantec trata la información del suscriptor con las finalidades de:</p> <ul style="list-style-type: none"> <li>• Habilitar y optimizar el funcionamiento de Norton Family;</li> <li>• Proporcionar asistencia o ayuda para la resolución de problemas;</li> <li>• Enviar al suscriptor información promocional de acuerdo con la autorización concedida por el suscriptor o según permita la legislación aplicable; y</li> <li>• Establecer la cuenta de Norton del suscriptor.</li> </ul> <p>2. Symantec trata los datos de dispositivos y software con las finalidades de:</p> <ul style="list-style-type: none"> <li>• Asegurar el correcto funcionamiento del producto y prestar los servicios solicitados por el suscriptor;</li> <li>• Administrar la licencia;</li> <li>• Evaluar y mejorar el porcentaje de éxito de instalación del producto;</li> <li>• Con fines de investigación y desarrollo para mejorar los productos y servicios de Symantec y proteger mejor la red, dispositivos, datos e identidad del suscriptor y los usuarios protegidos;</li> </ul> <p>3. La información del usuario protegido se trata con las finalidades de:</p> <ul style="list-style-type: none"> <li>• Identificar y autenticar al suscriptor y al usuario protegido para Symantec;</li> <li>• Ayudar al suscriptor a detectar cualquier uso indebido de los datos personales del usuario protegido; y</li> <li>• Comunicarse con el suscriptor y, con autorización del suscriptor, con el usuario protegido para prestar el servicio.</li> </ul> <p>4. La información de actividad del usuario protegido se trata con las finalidades de:</p> <ul style="list-style-type: none"> <li>• Ayudar al suscriptor a supervisar las actividades en línea del dispositivo del usuario protegido;</li> <li>• Limitar el daño causado por malware instalado;</li> <li>• Facilitar la aplicación de las normas definidas por el suscriptor sobre las actividades en línea del dispositivo del usuario</li> </ul>

	<p>bloquee para el usuario; términos de búsqueda que el usuario protegido utilice; aplicaciones que el usuario protegido instale o desinstale en sus dispositivos, si el suscriptor ha activado la monitorización de aplicaciones; el tiempo de uso del dispositivo del usuario protegido; *el nombre de perfil de usuario protegido, URL de perfil, edad, identificador de perfil en Facebook y vídeos visitados; vídeos que el usuario protegido visualice en YouTube o Hulu si el suscriptor ha activado la monitorización de vídeo.</p>	<p>protegido;</p> <ul style="list-style-type: none"> <li>• Permitir al suscriptor detectar si el usuario protegido está expuesto a amenazas mediante comunicaciones en línea o por SMS/MMS; y</li> <li>• Ayudar al suscriptor a proteger al usuario protegido ante dichas amenazas.</li> </ul> <p>Symantec utilizará además datos agregados, despersonalizados, anonimizados o no identificativos derivados de los datos recogidos, como las estadísticas, con las finalidades de:</p> <ul style="list-style-type: none"> <li>• Desarrollar investigaciones generales sobre ciberseguridad;</li> <li>• Mejorar la detección de malware y ciberamenazas, por ejemplo a través del análisis de muestras de archivos;</li> <li>• Realizar el seguimiento y publicación de informes sobre riesgos o tendencias de seguridad y robo de identidad; y</li> <li>• Realizar análisis estadísticos sobre implementación de productos, incluyendo el análisis de tendencias y comparativas en nuestra base de usuarios agregada.</li> </ul>
--	---	--

### Información adicional sobre Norton Family Premier

Si el suscriptor elige activar el servicio, Norton Family no permitirá al usuario protegido hacer públicos sus datos personales.

Cuando y en la medida en que lo permitan las leyes aplicables en el país o región en el que se encuentre el suscriptor, Symantec puede prestar un servicio de **Supervisión de Mensajes de Texto** que permita al suscriptor bloquear o supervisar los mensajes de texto (“SMS”) y multimedia (“MMS”) enviados a y desde el teléfono móvil del usuario protegido así como un **Servicio de Monitorización de la Ubicación**. La monitorización del intercambio de SMS y MMS o la ubicación y el uso de cualquier registro de dicha monitorización pueden estar limitados o prohibidos por las leyes locales aplicables al suscriptor. Es fundamental que el suscriptor consulte con las autoridades locales antes de activar esta característica.

Cuando el suscriptor active el Servicio de Monitorización de la Ubicación, Norton Family ejecutará la orden del suscriptor de utilizar el GPS para realizar un seguimiento y recoger la geolocalización del dispositivo móvil seleccionado por el suscriptor. Es necesario el consentimiento del suscriptor, y según el caso el consentimiento del usuario del dispositivo móvil o el consentimiento del titular de la responsabilidad parental sobre dicho usuario, para que Norton Family realice el seguimiento, recogida, utilización o revelación de la geolocalización del dispositivo seleccionado. El consentimiento o consentimientos pertinentes se recogen a través del portal en línea de Norton o, según proceda, en el producto y se confirman cuando el suscriptor introduce su información de pago de tarjeta para adquirir este servicio con Symantec en línea. Usted puede retirar cualquier consentimiento que haya dado en cualquier momento. Para obtener más información sobre cómo hacerlo consulte el apartado “Sus derechos de privacidad” del [Aviso de privacidad de Symantec - Norton](#). Tras la terminación del servicio se eliminará la información de cuenta del suscriptor relativa a este Servicio.

Una vez el suscriptor descargue la aplicación en el dispositivo seleccionado, Symantec recogerá la geolocalización de dicho dispositivo incluso cuando no se esté utilizando la aplicación. Únicamente revelaremos dicha información de geolocalización al suscriptor, para que este pueda localizar el dispositivo, y solo la trataremos con los fines operativos de prestar los servicios y funcionalidades solicitados por el suscriptor. El suscriptor no puede utilizar el servicio de monitorización de la ubicación del producto para supervisar los datos, ubicación, actividades u otros aspectos relacionados con un individuo respecto al que el suscriptor no tenga una responsabilidad parental. Los suscriptores en el Espacio Económico Europeo deben hablar con los usuarios protegidos bajo su responsabilidad parental, especialmente aquellos que sean mayores de 13 años, y tomar todas las medidas necesarias para asegurarse de que el usuario protegido en cuestión entienda lo que implica el uso del Producto y los Servicios asociados por parte del suscriptor. Cuando elija utilizar el Producto y los Servicios asociados, el suscriptor es el único responsable de cumplir todas las normativas y leyes aplicables a las relaciones del suscriptor con y responsabilidad parental sobre el usuario protegido.

#### Supervisión de Mensajes de Texto

La Supervisión de Mensajes de Texto está desactivada por defecto. El suscriptor ha de activar por separado la función de Supervisión de Mensajes de Texto e instalar Norton Family en el dispositivo móvil seleccionado para dicha supervisión. Cuando está activada, la Supervisión de Mensajes de Texto recoge la siguiente información del dispositivo seleccionado:

- El número de teléfono móvil del dispositivo que se está monitorizando y los números de teléfono móvil de otros dispositivos con los que el dispositivo intercambie comunicaciones por SMS y MMS;
- El contenido de los mensajes SMS recibidos o enviados por el dispositivo seleccionado (en el caso de las comunicaciones por MMS, Symantec no registrará ni capturará ningún contenido multimedia intercambiado, solo el hecho de que se produjo una comunicación por MMS);
- En caso de estar disponible, el nombre en la libreta de direcciones asociado en el dispositivo seleccionado con el número de teléfono que envíe comunicaciones por SMS y MMS al dispositivo seleccionado o que reciba dichas comunicaciones;
- Fecha/hora de la conversación;
- La ubicación del dispositivo seleccionado;
- El registro de mensajes SMS/MMS bloqueados incluidos números de teléfono de las partes y nombres asociados en caso de estar disponibles en la libreta de direcciones del dispositivo seleccionado.

Antes de comenzar a supervisar los mensajes SMS o MMS que un dispositivo móvil seleccionado por el suscriptor envíe o reciba, Symantec enviará una alerta SMS al dispositivo seleccionado avisando al usuario del dispositivo de que el producto se dispone a ejecutar la instrucción del suscriptor de registrar y supervisar el contenido de los mensajes SMS o MMS intercambiados en el dispositivo seleccionado. Si, tras recibir la alerta SMS, continúa el intercambio de mensajes SMS o MMS en el dispositivo seleccionado, comenzará el registro y monitorización de los mensajes con los fines descritos en el presente Aviso de acuerdo con las instrucciones del suscriptor. Symantec reenviará la misma alerta SMS al dispositivo seleccionado una vez al mes o cada vez que haya una nueva conversación.

Si el suscriptor elige bloquear todos los mensajes SMS o MMS o mensajes de una contraparte específica, avisaremos al usuario del dispositivo seleccionado y enviaremos un mensaje de texto a la contraparte indicando que el intercambio de mensajes se ha bloqueado y no puede entregarse el mensaje.