SOBRE LA SEGURIDAD DEL ALMACENAMIENTO EN LA NUBE

Máster interuniversitario de Seguridad de las tecnologías de la información y de las comunicaciones

Autor: Andrés Galmés Hernández

Directora: María Francisca Hinarejos Campos

Universitat Oberta de Catalunya

Enero de 2016

A ses meves tres al·lotes, Susana, Nura i Martina, que sense es seu suport i paciència no hagués pogut acabar mai aquesta feina.

La ventura va guiando nuestras cosas mejor de lo que acertáramos a desear; porque ves allí, amigo Sancho Panza, donde se descubren treinta o pocos más desaforados gigantes, con quien pienso hacer batalla…

Mire vuestra merced –respondió Sancho– que aquellos que allí se parecen no son gigantes, sino molinos de viento…

Bien parece –respondió don Quijote– que no estás cursado en esto de las aventuras: ellos son gigantes; y si tienes miedo quítate de ahí,… que yo voy a entrar con ellos en fiera y desigual batalla.

Don Quijote de La Mancha

Miguel de Cervantes

FICHA DEL TRABAJO FINAL

Título del trabajo:	Sobre la seguridad del almacenamiento en la nube
Nombre del autor	Andrés Galmés Hernández
Nombre del consultor:	María Francisca Hinarejos Campos
Fecha de entrega (mm/aaaa):	01/2016
Área del Trabajo Final:	Comercio electrónico
Titulación:	Máster interuniversitario de Seguridad de las tecnologías de la información y de las comunicaciones (MISTIC)

Resumen:

Los servicios y productos de almacenamiento de datos en la nube permiten a sus usuarios guardar y compartir cualquier tipo de documento y archivo desde cualquier dispositivo conectado a Internet. Estos almacenes de información son un objetivo para cualquiera que pretenda hacerse con información confidencial o privada. Existen diferentes amenazas tales como violación y pérdida de datos que ponen en riesgo la seguridad de la información almacenada en la nube.

Es importante señalar que el usuario debería ser consciente de las garantías de seguridad que estos ofrecen. Para tomar la decisión correcta en relación al servicio que se ajusta a las necesidades de cada usuario, una buena práctica consiste en analizar las medidas de seguridad de los productos de almacenamiento en la nube. Es importante considerar metodologías de análisis que permitan estudiar la seguridad de uno o varios productos y comparar sus resultados.

El presente trabajo se centra en analizar la seguridad de productos pertenecientes a varios proveedores de distintos ámbitos geográficos y jurídicos (Yandex.Disk, CloudMe y Google Drive). Los resultados demuestran que estos productos tienen carencias en cuanto a la implementación de los requisitos de seguridad. Este hecho los expone a importantes amenazas.

Abstract:

Cloud storage products and services enable users to store and share data from any device connected over Internet. This data store is an attractive target for those who seek to get users' confidential information and private data. There are threats such as data breaches and data loss, which can compromise the security of information stored in the cloud.

Importantly, users should be aware of the guarantees of the cloud security offered by providers. In order to make the right decision on the service to meet users' needs, the best practice is to analyze the cloud security measures. It is important to consider methodologies that enable a comparative analysis of the cloud storage security for different products and services.

The present research focuses on analyzing the cloud security of products from several providers located in different geographical areas, administrative and legal frameworks (Yandex.Disk, CloudMe and Google Drive). The results show that the products have weaknesses regarding the implementation of security requirements. Therefore, these products are exposed to important threats.

Palabras clave:

nube

servicio

almacenamiento
seguridad
amenazas
análisis

Tabla de contenido

1. Introducción

La **computación en la nube** se ha convertido en el nuevo paradigma de computación para empresas, la nueva forma de hacer las cosas, que permite ofrecer servicios informáticos en la red de forma ágil y flexible [1] [3], abordar el rápido crecimiento de dispositivos conectados a la *web* y la gestión de cantidades masivas de información [2]. Los servicios ofrecidos por la nube permiten la prestación de hardware, sistemas, software o almacenamiento por parte de un proveedor, con independencia de dónde se encuentren alojados los sistemas de información que los soportan y de forma completamente transparente a sus usuarios [2] [3].

Uno de los servicios ofrecidos por la nube es el de **almacenamiento de datos** (*cloud storage* en inglés). Este servicio permite a los proveedores de servicio almacenar cantidades masivas de datos de sus clientes en sus centros de datos, siendo transparente para el usuario final la localización exacta de su información, que puede estar situada en cualquier lugar del planeta [3]. Entre sus ventajas están las de cubrir las necesidades crecientes de almacenamiento de información de los usuarios, recortar drásticamente los costes de almacenamiento inherentes a los dispositivos tradicionales (discos duros, *CD*, *DVD*, etc.), almacenar y acceder a los datos desde diferentes dispositivos conectados a Internet (ordenadores, teléfonos móviles, tabletas o videoconsolas) y el mantenimiento de los datos proporcionado por la propia nube (alta disponibilidad, *backup*, etc.).

Una de las mayores barreras en la adopción del almacenamiento en la nube es la **seguridad** [6]. Los **problemas de seguridad** no son muy diferentes a los de cualquier entorno TI, sin embargo, debido a su propia naturaleza (modelos de servicio y operacionales, tecnologías usadas, etc.) la computación en la nube, y por tanto los servicios de almacenamiento, presenta **riesgos** nuevos para sus usuarios, como pueden ser la pérdida o violación de datos privados y confidenciales (uno puede imaginarse el problema que supondría para un hospital y sus pacientes la pérdida de historias clínicas o su acceso no autorizado). La gran cantidad de información almacenada por millones de usuarios, provoca que estos servicios sean un objetivo muy atractivo para quien pretenda robar o acceder a información valiosa; enfrentándose así a **ataques** continuos que ponen en **riesgo la seguridad de los datos**. Estos problemas de seguridad hacen dudar a los usuarios, especialmente a las empresas, a la hora de confiar sus datos a los servicios de almacenamiento en la nube.

Es muy importante seleccionar un producto adecuado a los requisitos seguridad de cada usuario. Actualmente, existen **diferentes productos**, desde los orientados a los usuarios particulares, que se limitan a almacenar sus recibos de la compra o el proyecto final de máster del MISTIC, hasta las grandes empresas que pueden almacenar documentos secretos sobre su estrategia empresarial, datos de sus clientes o el diseño del último chip para manipular las emisiones de los motores diésel que fabrican. Sin embargo, para poder conocer qué producto seleccionar es necesario realizar un **análisis** previo **de seguridad**, con el fin de comprobar si se adapta a las necesidades de los usuarios.

El **objetivo** del presente trabajo es el de **analizar la seguridad** de tres productos de almacenamiento en la nube, pertenecientes a tres proveedores de distintos ámbitos geográficos y jurídicos, como son Yandex.Disk, CloudMe y Google Drive. Para conseguirlo, se propone un conjunto de tareas cuya descripción y alcance se irán viendo a lo largo del documento.

En **primer lugar**, se realizará una introducción a la computación en la nube, donde se revisarán las características esenciales definidas por el *National Institute of Standards and Technology* (NIST) de EE.UU., los diferentes modelos de despliegue (*nube pública, nube privada, nube comunitaria* y *nube híbrida*) y los modelos de servicios (*IaaS, PaaS* y *SaaS*). En **segundo lugar**, se revisarán las características, clasificación y evolución del almacenamiento en la nube.

En **tercer lugar**, se estudiará la seguridad del almacenamiento en la nube. Se empezará revisando sus principales amenazas, según los estudios de la *Cloud Security Alliance* (CSA) y de la *European Union Agency for Network and Information Security* (ENISA). A continuación, se estudiarán los aspectos de seguridad relevantes a tener en cuenta, tomando como base trabajos del Instituto Nacional de Ciberseguridad (INCIBE) y del *Fraunhofer Institute for Secure Information Technology* (SIT), dando como resultado una serie de requisitos destinados a mitigar el impacto de las amenazas sobre los datos de los usuarios, en términos de su confidencialidad, integridad y disponibilidad. Estos requisitos servirán de base para el estudio de seguridad de los productos seleccionados.

Finalmente, a partir de los resultados obtenidos en los apartados anteriores, se procederá al análisis de la seguridad de Yandex.Disk, Google Drive y CloudMe. Se estudiará cómo resuelven el cumplimiento de los requisitos de seguridad establecidos para sus principales procesos (registro, *login*, transmisión, etc.). Como resultado del análisis, se verán las diferentes alternativas que los diferentes proveedores aplican y una comparativa del cumplimiento de los requisitos.

2. Tareas y riesgos del proyecto

Cualquier definición y planificación de tareas es vital para la consecución de un proyecto de ingeniería. Sin conocer previamente qué quiere obtenerse, el tiempo disponible y cuáles son los principales pasos y tareas para alcanzar un objetivo, es muy complicado finalizar con éxito cualquier trabajo. Entre estas tareas debe contemplarse la gestión de riesgos y problemas que surgen a lo largo de la vida de un proyecto, que pueden incluso derivar en una modificación del alcance inicial. En la siguiente tabla, se definen las principales tareas planificadas para la realización del presente trabajo.

Tareas principales	Descripción de tareas
Definir proyecto	Determinación de alcance del proyecto y su planificación.
Introducción a la computación y el almacenamiento en la nube	
Introducir la computación en la nube	Definir las principales características y los modelos de la computación en la nube.
Introducir el almacenamiento en la nube	Definir el almacenamiento en la nube, cómo se clasifica y los beneficios que aporta.
Estudiar la seguridad del almacenamiento en la nube	
Describir amenazas de seguridad	Revisar y describir las principales amenazas de seguridad a las que se expone el almacenamiento en la nube.
Aspectos y requisitos de seguridad	Revisar y analizar aspectos relevantes de seguridad en la nube. Definir requisitos de seguridad para mitigar impacto de ataques.
Análisis de seguridad de servicios y productos de almacenamiento en la nube	
Preparar análisis	Definir metodología de análisis de seguridad. Seleccionar los productos de almacenamiento en la nube a analizar. Seleccionar procesos de los productos a estudiar y los requisitos para los que se quiere analizar su cumplimiento.
Analizar Yandex.Disk	Analizar la seguridad del producto ruso Yandex.Disk.
Analizar CloudMe	Analizar la seguridad del producto sueco CloudMe.
Analizar Google Drive	Analizar la seguridad del producto estadounidense Google Drive.
Comparar resultados	Comparar los resultados del análisis de cada producto y sacar conclusiones al respecto.
Seguimiento	
Realizar entregas parciales del trabajo	Esta tarea se realizará durante todo el proyecto, con el fin de ir supervisando su desarrollo.
Finalización	
Finalizar proyecto	Finalizar y entregar la memoria del proyecto, la presentación y el video.

TABLA 1 – PRINCIPALES TAREAS DEL PROYECTO

Los principales riesgos detectados en este trabajo están relacionados, principalmente, con el tiempo disponible por parte de su autor. En la siguiente tabla pueden verse estos riesgos y las acciones que se llevarán a cabo para mitigarlos.

Riesgo	Probabilidad de ocurrencia	Acciones / Contingencias
Que el alcance resulte demasiado amplio para el tiempo disponible.	Media	Reducir el alcance o esfuerzo dedicado a tareas “menos relevantes” para el resultado final del proyecto.
No encontrar la información suficiente durante el estudio de alguna de las soluciones.	Baja	Diferentes opciones que podrían llevarse a cabo son: realizar pruebas de concepto para poder obtener la información necesaria.

Riesgo	Probabilidad de ocurrencia	Acciones / Contingencias
Desconocimiento de la tecnología de computación en la nube.	Media	Estudiar conceptos que permitan iniciar el análisis de los productos y servicios seleccionados.
Compromisos de carácter familiar o laboral.	Alta	Reducir el alcance o esfuerzo dedicado a tareas “menos relevantes” para el resultado final del proyecto.

TABLA 2 – RIESGOS DEL PROYECTO

3. Introducción a la computación en la nube

El NIST define la computación en la nube como "*un modelo para permitir el acceso por red, de forma ubicua, práctica y bajo demanda, a un conjunto compartido de recursos de computación configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser suministrados y desplegados rápidamente con una mínima gestión o interacción con el proveedor del servicio. Este modelo se compone de cinco características esenciales, tres modelos de servicio y cuatro modelos de despliegue*" [4]. Un resumen de este modelo de NIST puede verse en la imagen de la Figura 1, cuyos componentes se describirán más adelante.

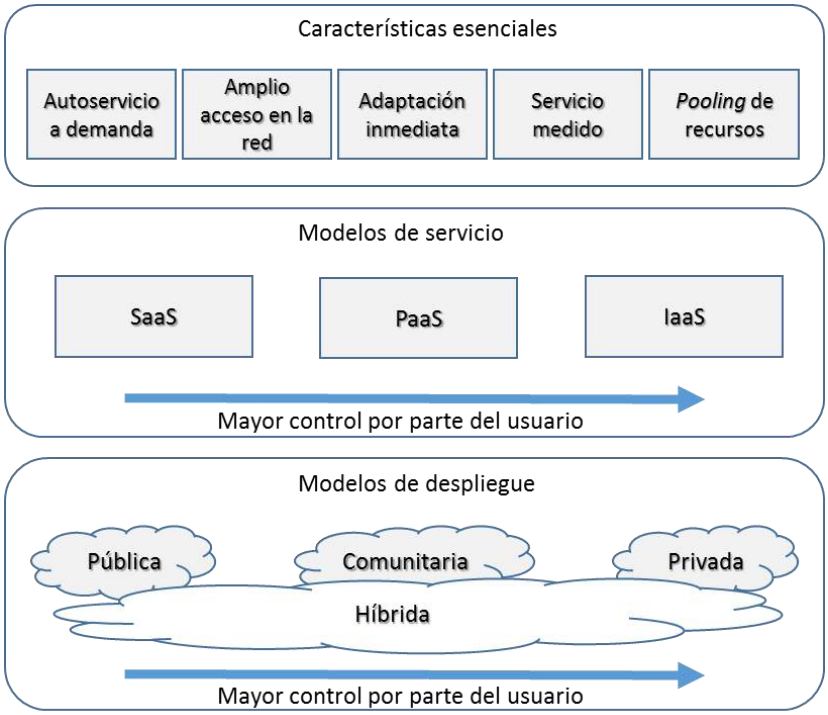


FIGURA 1 – MODELO DE LA NUBE DE NIST [5]

3.1 Características esenciales

El modelo de NIST identifica cinco características esenciales que deben cumplir los servicios en la nube [5], las cuales se introducen a continuación.

Autoservicio a demanda

Los usuarios de los servicios en la nube han de poder ajustar su capacidad necesaria de forma unilateral, sin la necesidad de requerir intervención humana por parte del proveedor del servicio [4].

Amplio acceso en la red.

El acceso a los servicios de la nube debe realizarse a través de la red y mecanismos estándar, usando todo tipo de dispositivos: teléfonos móviles, portátiles, ordenadores personales, *tablets*, servidores, etc. [4].

Adaptación inmediata

La capacidad requerida puede provisionarse rápida, elástica y automáticamente, para seguir las variaciones de la demanda por parte de los usuarios. Desde el punto de vista del usuario, los recursos parecen ilimitados, pudiendo disponer de cualquier cantidad en cualquier momento [4].

Servicio medido

Los sistemas en la nube automáticamente controlan y optimizan los recursos utilizados, a través de la capacidad de medición en el nivel de abstracción apropiado para el tipo de servicio ofrecido (almacenamiento, procesamiento, ancho de banda, cuentas de usuarios activas, etc.). El uso de recursos puede ser monitorizado, controlado y reportado, proporcionando transparencia tanto para el proveedor como para el usuario del servicio [4].

***Pooling* de recursos**

Los recursos de computación del proveedor se agregan (*pool* en inglés) para poder servir a múltiples usuarios. La agregación incluye recursos físicos y virtuales, asignados dinámicamente y reasignados según las demandas de los usuarios del servicio. Existe cierta sensación de independencia de la localización por parte del usuario, ya que éste, generalmente, no tiene ningún tipo de control o conocimiento de dónde se encuentran los recursos; aunque puede especificar la localización a un nivel superior de abstracción (país, área geográfica, centro de datos, etc.). Ejemplos de estos recursos incluyen: almacenamiento, procesamiento, memoria, ancho de banda de red y máquinas virtuales [4].

3.2 Modelos de servicio

Los modelos de servicios definidos por el NIST pueden clasificarse principalmente según ofrezcan infraestructura, plataforma o software como servicio, los cuales se introducen a continuación [4].

Infraestructura como Servicio (**IaaS** – del inglés *Infrastructure as a Service*)

El proveedor del servicio presta una **infraestructura** a sus usuarios, la cual incluye procesamiento, almacenamiento, redes y otros recursos fundamentales de computación, sobre los cuales el consumidor es capaz de desplegar y ejecutar software arbitrario, que puede incluir sistemas operativos y aplicaciones. El usuario no administra ni controla la infraestructura subyacente de la nube (*hypervisor*, almacenamiento, hardware y red), en cambio, sí tiene control sobre los sistemas operativos, almacenamiento virtualizado, aplicaciones implementadas y el control, posiblemente, limitado de algunos componentes de red. Ejemplos de proveedores y productos IaaS son: Amazon Elastic Compute Cloud (Amazon EC2), Google Compute Engine, Oracle Compute Cloud Service y Microsoft Azure.

Plataforma como Servicio (**PaaS** – *Platform as a Service*)

El proveedor del servicio presta una **plataforma** de procesamiento a sus usuarios, para que puedan desplegar y ejecutar sus propios servicios o aplicaciones sobre ésta. El usuario no administra ni controla la infraestructura (sistema operativo, *hypervisor*, almacenamiento, hardware y red), pero tiene el control sobre las aplicaciones instaladas y su configuración. En ocasiones, los proveedores de PaaS suministran las herramientas de desarrollo necesarias para la plataforma. Ejemplos de proveedores y productos PaaS son: Google App Engine, Amazon AWS Elastic Beanstalk, Oracle Cloud Platform for Data Management y Red Hat OpenShift.

Software como Servicio (**SaaS** – *Software as a Service*)

El usuario usa las aplicaciones que ofrece el proveedor del servicio en la nube a través de Internet. Estas aplicaciones son accesibles desde varios dispositivos a través de clientes ligeros, como puede ser un navegador *web*. El usuario no administra ni controla la infraestructura en la que se basa el servicio que utiliza. El rango de aplicaciones de un SaaS comprende: servidores de correo electrónico,

editores de documentos, redes sociales, almacenamiento, etc. Es común que los proveedores SaaS corran sus aplicaciones sobre servicios IaaS o PaaS ofrecidos por otros como, por ejemplo, el proveedor de servicio multimedia por *streaming* Netflix (SaaS), que corre sobre servicios IaaS y PaaS de Amazon AWS. Otros ejemplos de proveedores y productos SaaS son: Google Drive, Google Maps, Yahoo Mail, Yandex.Disk, CloudMe y Salesforce.com con su CRM en la nube.

Es habitual referirse a estos tres modelos como el **modelo SPI** (SaaS, PaaS, IaaS). Por otro lado, se han propuesto otros modelos de servicio, que pueden ser considerados **especializaciones** de los anteriores, como pueden ser [5]: Datos como Servicio (DaaS), Seguridad como Servicio (SECaaS), Monitorización como Servicio (MaaS), Identidad como Servicio (IDaaS), Comunicaciones como Servicio (CaaS), Red como Servicio (NaaS – *Network as a Service*), etc.

3.3 Modelos de despliegue

Según la titularidad de las infraestructuras en la nube, estas pueden clasificarse en públicas, privadas, comunitarias o híbridas [4].

Nube pública.

La infraestructura de la nube está **disponible para el público en general** a través de Internet. Suele ser propiedad de un proveedor que gestiona la infraestructura y los servicios que se ofrecen. Algunas de sus **ventajas** son su escalabilidad, eficiencia del uso de sus recursos y el ahorro de tiempo y costes de mantenimiento [14]. Entre sus **desventajas** destacan el hecho de que la infraestructura es compartida por multitud de usuarios, los cuales no conocen el resto de servicios con los que comparten recursos, y la dependencia en la seguridad suministrada por el proveedor [14].

Nube privada.

La infraestructura de la nube se provisiona para el **uso exclusivo de una única organización** con múltiples usuarios (áreas de negocio, departamentos, etc.). Puede pertenecer, ser gestionada y operada por la misma organización, terceros o una combinación de ambos. Sus sistemas pueden encontrarse en las mismas instalaciones de la organización o en las de un tercero. Algunas de sus **ventajas** pueden ser su adaptación al cumplimiento de las políticas internas de seguridad y privacidad de la compañía, el control total de los recursos por parte de la organización y la facilidad en el trabajo colaborativo entre usuarios y sedes distribuidas de la empresa [14]. Entre sus **desventajas** destacarían su elevado coste material (requieren de los mismos recursos de personal, gestión, mantenimiento y capital, que los centros de datos tradicionales, además de sistemas de virtualización, software dedicado y herramientas de gestión), una elevada dependencia de la infraestructura contratada y un retorno de inversión lento por su carácter de servicio interno [14].

Nube comunitaria.

La infraestructura de esta nube es **compartida por varias organizaciones** de una comunidad específica que comparten requisitos de servicio (seguridad, jurisdicción, cumplimiento, políticas, misión, etc.). Puede estar gestionada y operada por una o más de las organizaciones involucradas, por terceros o una combinación de ambos. Los costes se reparten entre sus componentes. Sus sistemas pueden encontrarse en las mismas instalaciones de las organizaciones participantes, en las de un tercero o una combinación de ambas opciones. Algunas de sus **ventajas** pueden ser su adaptación al cumplimiento de las políticas internas de seguridad y privacidad de la compañía, la reducción de costes al compartir la infraestructura y los recursos y un retorno más rápido de inversión que en el caso de las privadas [14]. Entre sus **desventajas** destacaría el hecho de que su seguridad depende del anfitrión de la infraestructura [14].

Nube híbrida.

La infraestructura es una **composición** de dos o más de los **modelos** anteriores (pública, privada o comunitaria), que permanecen como entidades únicas, pero que coexisten por medio de tecnología que permite compartir datos y aplicaciones entre cada una de ellas [4]. El almacenamiento en la nube híbrido cuenta con las ventajas y desventajas que las relativas a los tipos que incluyen la infraestructura [14].

4. Almacenamiento en la nube

El **almacenamiento de datos** es uno de los principales servicios de la nube y uno de los más populares hoy en día [18]. Usando tecnología de computación en la nube, permite a sus proveedores suministrar almacenamiento *virtualizado* bajo demanda y almacenar cantidades masivas de datos de sus usuarios en redes de centros de datos distribuidos, siendo transparente para el usuario final la localización exacta de su información, que puede estar situada en cualquier lugar del planeta [3] [16].

Dicho lo anterior, en este apartado se verá primero, de forma resumida, cuál ha sido la evolución de la tecnología desde la invención del disco duro hasta el almacenamiento en la nube, tal y como se conoce en la actualidad. Seguidamente, se introducirán sus principales ventajas e inconvenientes de cara a los usuarios de este servicio. Se dará una clasificación de los tipos de almacenamiento en la nube existente, junto con su comparativa con respecto a una serie de características. Para finalizar, veremos qué interfaces y API son las más comunes hoy en día para el acceso a los datos en la nube.

4.1 Evolución del almacenamiento en la nube

La evolución del almacenamiento en la nube no es más que la continuación de la evolución del almacenamiento de datos, que se remonta al siglo XIX con el invento de las tarjetas perforadas. Pero no nos vayamos tan atrás, sino hasta 1956, cuando IBM desarrolla el primer disco duro:

- **1956** – IBM desarrolla el primer disco duro con capacidad para 3,75MB. Aun no existe tecnología de acceso a datos remotos.
- **1969** – Nace la red ARPANET, desarrollada por el departamento de defensa de EE.UU. Ya se puede acceder a los datos situados en otro equipo de forma remota.
- **1979** – EMC2 empieza a promocionar la primera nube privada. Los dispositivos de almacenamiento se encuentran dentro de las organizaciones.
- **1982** – IBM desarrolla el adaptador Ethernet, que permite conexiones rápidas y a bajo coste para acceder de forma *online* al almacenamiento remoto.
- **Década de 1990** – Realización de backups de forma *online*. Durante el surgimiento de las empresas *punto-com*, aparecen los primeros servicios de *backup online* a través de Internet. Cientos de empresas ofrecen el servicio.
- **1996** – La armada estadounidense lanza el proyecto Ethernet denominado IT-2, para el desarrollo de una red con el objetivo de compartir información de forma segura.
- **2006** – Surge Amazon AWS S3. Puede decirse que Amazon lanza la computación en la nube tal y como se conoce hoy en día. S3 es su servicio de almacenamiento en la nube, que aún continúa ofreciendo.
- **2007** – Aparece la primera reléase de Dropbox y con éste el almacenamiento en la nube personal. Aplica un modelo de servicio gratuito, donde los usuarios pueden ocupar cierta cantidad de datos antes de empezar a cobrar por el servicio. Usa el servicio S3 de Amazon para almacenar los datos de sus usuarios.
- **2008** – Se pone a disposición del público de 38 países el producto de almacenamiento en la nube de Microsoft, SkyDrive, precursor de OneDrive.
- **2012** – Google lanza su servicio Google Drive, como evolución de Google Docs. En el año 2013 ya tenía unos 120 millones de usuarios.
- **2015** – Existen multitud de proveedores que ofrecen almacenamiento en la nube y millones de usuarios que lo utilizan.

4.2 Ventajas e inconvenientes

Existe una serie de ventajas e inconvenientes importantes para los usuarios de los servicios de almacenamiento en la nube. Algunas de las **ventajas** que pueden destacarse son [5]:

- Ofrece a las pequeñas compañías **acceso a bajo coste** a capacidades que las grandes compañías gestionan internamente, permitiendo así que sean más competitivas.

- Los proveedores del almacenamiento en la nube también ofrecen a los usuarios individuales acceso a estas capacidades, ofreciéndoles, además, **planes gratuitos** de almacenamiento.
- Aportan beneficios a sus usuarios, individuales y compañías, al **externalizar** el hardware, software, mantenimiento y gestión del almacenamiento de datos.
- Los usuarios pueden fácilmente **incrementar la capacidad** de su almacenamiento.
- Los proveedores de almacenamiento realizan ***backups*** de datos de forma transparente para sus usuarios.
- Permite a sus usuarios el **acceso a los datos** en cualquier momento desde cualquier lugar.
- Se acerca al 100% de **uso del almacenamiento**, eliminando las grandes cantidades de almacenamiento infrautilizado que debe soportar el almacenamiento tradicional, para anticipar el crecimiento y los picos de carga [11].
- Algunos estudios demuestran que permite disminuir el **consumo eléctrico**, cuando una empresa contrata el servicio de almacenamiento en la nube a un proveedor externo.

Entre los principales **inconvenientes** pueden incluirse:

- Si no existe **conexión a Internet**, los usuarios no pueden acceder a sus datos.
- La preocupación que genera a los usuarios en cuanto a la **seguridad** y **privacidad** de sus datos [5].
- El desconocimiento para la mayoría de usuarios de la **localización de sus datos**.

4.3 Clasificación del almacenamiento en la nube

De la misma manera que en la computación en la nube, el almacenamiento en la nube puede clasificarse según su modelo de despliegue. Es decir, podría clasificarse de la siguiente forma [11]:

1. Almacenamiento en la nube público.
2. Almacenamiento en la nube privado.
3. Almacenamiento en la nube híbrido.

Almacenamiento en la nube público.

El servicio de almacenamiento lo presta y gestiona un proveedor de servicios en un modelo de **nube pública** (con sus ventajas e inconvenientes). Normalmente, estos servicios son contratados por los usuarios mediante el pago por uso de gigabyte almacenado y transferido, dependiendo del proveedor [11]. La mayoría de proveedores dan la posibilidad de usar sus servicios de forma gratuita, pero con limitaciones en la capacidad de almacenamiento (por ejemplo, Google Drive y Yandex.Disk ofrecen 15 GB y 10 GB respectivamente de forma gratuita).

Este tipo de almacenamiento, está diseñado para poder trabajar con **cantidades masivas de usuarios**, permitiendo el aislamiento de datos, acceso y seguridad por cada usuario. El tipo de contenido que normalmente almacenan comprende datos estáticos de aplicaciones que no son críticos, archivos que necesitan estar disponibles desde cualquier lugar, así como *backups* de datos y de recuperación de desastres, entre otros. Sin embargo, no es demasiado conveniente para trabajar con contenido dinámico que cambia constantemente. Una de las principales preocupaciones de cara a sus usuarios es el hecho de que delegan el control y la seguridad de sus datos a un tercero, desconociendo dónde se almacenarán realmente, lo que puede ser un problema de cara al cumplimiento de la legislación vigente [11] [14]. Otras de los problemas que presentan es su bajo rendimiento según [11].

Dentro de este modelo, puede incluirse el **almacenamiento en la nube personal o móvil**. Puede ser visto como un subconjunto del público, que provee a los usuarios particulares de un servicio de almacenamiento, acceso, sincronización y compartición de datos, fotos, videos y otros tipos de archivos desde cualquier parte y dispositivo con una conexión a Internet. Ejemplos de proveedores de estos servicios son Google Drive, Dropbox y Apple iCloud [11] [12].

Almacenamiento en la nube privado.

El servicio de almacenamiento se provisiona, en un modelo de **nube privada**, únicamente por y para una organización, con recursos de almacenamiento propios o en las instalaciones de un proveedor especializado. Esto permite que los datos sensibles para sus usuarios residan en las instalaciones de la organización, lo que implica una mejora en cuanto a seguridad y privacidad de la información, con respecto al modelo público [11] [14]. Sin embargo, sus requisitos de escalabilidad son más limitados [11], ya que el almacenamiento en la nube privado se parece más a un centro de datos tradicional con limitaciones de espacio y costes.

Almacenamiento en la nube híbrido.

El servicio de almacenamiento se provisiona mediante un modelo de **nube híbrida**, donde los datos críticos podrían almacenarse en la nube privada o instalaciones de la organización, mientras que el resto puede guardarse en la nube pública. Sin embargo, para que pueda funcionar, deben cumplir con ciertos requisitos claves: comportarse como un almacenamiento homogéneo, ser virtualmente transparente y contar con mecanismos que mantengan los datos más usados frecuentemente en la nube privada o instalaciones de la organización, mientras mueve el resto hacia la nube pública. Esto implica definir políticas para decidir cuándo mover y extraer los datos hacia y desde la nube pública [11].

Para finalizar, en la Tabla 3, puede verse un **resumen** con la comparativa entre los diferentes tipos de almacenamiento, con respecto a las siguientes **características** [11], la cuales deben tenerse en cuenta a la hora de seleccionar un tipo u otro de almacenamiento en la nube:

- Escalabilidad.
- Seguridad.
- Rendimiento.
- Fiabilidad.
- Coste.

Características	Almacenamiento en la nube público	Almacenamiento en la nube privado	Almacenamiento en la nube híbrido
Escalabilidad	Muy alto.	Limitado por los recursos de la organización.	Muy alto.
Seguridad	Bueno, aunque depende de las medidas de seguridad del proveedor del servicio.	El más seguro, puesto que todo el almacenamiento se encuentra en las instalaciones de la organización.	Muy seguro. Las opciones de integración añaden una capa adicional de seguridad.
Rendimiento	Bajo a medio.	Muy bueno.	Bueno, ya que el contenido activo se cachea en las instalaciones.
Disponibilidad	Media. Depende de la conectividad con Internet y la disponibilidad del proveedor del servicio.	Alta, ya que todos los recursos se encuentran en las instalaciones de la organización.	Media a alta, puesto que el contenido en caché se mantiene en las instalaciones de la organización, pero depende de la conectividad con el proveedor de almacenamiento público.

Características	Almacenamiento en la nube público	Almacenamiento en la nube privado	Almacenamiento en la nube híbrido
Coste	Muy bueno. Tienen un modelo de pago medido, ofreciendo servicios gratuitos en muchos casos, y no es necesario tener ningún tipo de infraestructura de almacenamiento por parte de los usuarios.	Bueno, pero requiere recursos en las instalaciones de la organización, como un centro de datos, gasto eléctrico, aire acondicionado, mantenimiento, etc.	Mejor que el privado, ya que permite mover recursos de almacenamiento hacía un modelo público de pago medido.

TABLA 3 – COMPARATIVA ENTRE LOS DIFERENTES TIPOS DE ALMACENAMIENTO EN LA NUBE

4.4 Acceso al almacenamiento en la nube

El acceso al almacenamiento en la nube puede hacerse desde múltiples tipos de dispositivos: ordenadores personales, móviles, tabletas, televisiones inteligentes, etc. Para esto, es necesario que el proveedor ofrezca una serie de interfaces y API, con el fin de que sus clientes puedan consumir sus servicios.

La mayoría de proveedores en la nube ofrecen acceso a sus servicios de almacenamiento mediante el uso de **API RESTful** sobre el protocolo HTTP, lo que permite trabajar con sistemas heterogéneos, abstrayendo a los desarrolladores de aplicaciones y a sus usuarios de la complejidad de los sistemas que componen un servicio de almacenamiento en la nube. En la actualidad, existen diferentes implementaciones para estas API, aunque se considera la implementación de Amazon como un estándar de facto [9]. Por otro lado, la *Storage Networking Industry Association* (SNIA) ha publicado un estándar internacional, llamado *Cloud Data Management Interface* (CDMI), pensado para los desarrolladores de aplicaciones de almacenamiento en la nube [15]. Normalmente, los clientes de almacenamiento ofrecidos por los propios proveedores hacen uso de estas API.

Por otro lado, algunos proveedores permiten el acceso a los datos mediante el protocolo **WebDAV**, que es una extensión de HTTP. Esto hace posible que, cuando no se puede instalar la aplicación nativa del proveedor o no se quiere tener una copia en local de los datos, se pueda acceder mediante un cliente WebDAV al almacenamiento. Ejemplos serían el propio Explorer de Microsoft Windows, Nautilus 3.6 o superior de Gnome en Linux, además de otras aplicaciones de terceros [38]. Finalmente, todos los proveedores ofrecen una **consola *web*** que permite a los usuarios del servicio el acceso a sus datos almacenados, además de la gestión de sus cuentas, registro, etc.

5. Seguridad del almacenamiento en la nube

Los servicios de almacenamiento en la nube recogen y guardan información relevante de muchas fuentes distintas de todo el mundo, con lo que son un objetivo muy interesante para cualquier atacante, desde el estudiante que quiere copiar el trabajo de clase de un compañero hasta agencias nacionales de inteligencia. Por otro lado, junto al avance de las tecnologías de almacenamiento en la nube, han aparecido nuevas **vulnerabilidades y amenazas** de seguridad [14] [22], que pueden ser aprovechadas por los atacantes y que de materializarse pondrían en riesgo los datos de sus usuarios y la credibilidad del proveedor. Algunas de estas amenazas se describen en este capítulo, además de los aspectos y requisitos de seguridad que pueden mitigar su impacto y que conforman la base para el análisis de los productos de almacenamiento en capítulos posteriores.

5.1 Amenazas de seguridad del almacenamiento en la nube

En el presente apartado, se introducen algunas de las amenazas a las que se enfrentan los productos de almacenamiento en la nube, descritas principalmente en el trabajo realizado por la *Cloud Security Alliance* (CSA), conocido como *The Notorious Nine Cloud: Computing Top Threats in 2013* [22], así como en otros trabajos e informes de la ENISA en [24] y [25] y del INCIBE de España en [14]. Las amenazas son:

- Violación de datos.
- Pérdida de datos.
- Secuestro de cuenta o servicio.
- Interfaces y API de gestión inseguras.
- Denegación de servicio: DoS y DDoS.
- Personal interno malicioso.
- Fallos en la tecnología de compartición – fallo de aislamiento.
- Software vulnerable.
- Cumplimiento de la legislación vigente.
- Ataques a la red.
- Robo o pérdida de dispositivos.

En los siguientes subapartados, para cada una de las amenazas citadas, se dará una pequeña descripción, indicando la fuente de la que se ha tomado y su impacto sobre la seguridad y privacidad de los datos en términos de las dimensiones de confidencialidad, autenticación, disponibilidad e integridad de la información.

5.1.1 Violación de datos (T1)

Fuente: CSA

Impacto: Confidencialidad, disponibilidad, integridad

La **violación de datos** puede definirse como la violación de la seguridad en la que se copian, transmiten, visualizan, roban, destruyen, alteran o usan de forma no autorizada datos sensibles, protegidos o confidenciales, los cuales pueden estar almacenados, transmitiéndose o ser procesados de cualquier otra forma [20] [21].

Ejemplos recientes de violaciones de datos pueden ser: el ataque contra *Apple iCloud* en 2014, conocido como *Celebrity Photo Leak* y que puso al descubierto imágenes íntimas de algunos personajes de la farándula, o el que se produjo contra la compañía *Anthem* en 2015, que permitió a los atacantes el acceso a datos de salud de millones de sus clientes norteamericanos [16].

5.1.2 Pérdida de datos (T2)

Fuente: CSA

Impacto: Disponibilidad

La **pérdida de datos** puede definirse como la destrucción de la información, de forma intencionada (por ejemplo, un ataque terrorista) o accidental, que será permanente a menos que el proveedor del servicio haya implementado medidas eficientes de replicación, *backup* y restauración de datos [22]. También se considera pérdida de datos el caso en que un usuario pierde u olvida las claves con las que cifró su información antes de subirla a la nube, ya que posteriormente, no podrá descifrar ni recuperar sus datos [22].

Ejemplo de pérdida de datos en un proveedor de almacenamiento en la nube lo tenemos en [30] y [31]. En agosto de 2015, una tormenta eléctrica tumbó un centro de datos de Google en Bélgica, lo que supuso la pérdida momentánea de datos para una parte de sus usuarios europeos. Posteriormente, los datos pudieron ser recuperados gracias a las copias que Google dispone en otros centros. Sin embargo, cerca del 0.000001% de información se ha perdido permanentemente.

5.1.3 Secuestro de cuenta o servicio (T3)

Fuente: CSA, ENISA

Impacto: Confidencialidad, autenticación, disponibilidad, integridad

Si un atacante es capaz de **hacerse con las credenciales** de un usuario o proveedor (mediante *phishing*, ingeniería social, *eavesdroping* en una *WiFi* pública o aprovechando vulnerabilidades del software), podrá espiar sus actividades y transacciones, violar sus datos, devolver información falsa, redirigir las peticiones a sitios maliciosos y usar la potencia de la nube para lanzar nuevos ataques o almacenar información ilícita, entre otros [22] [23].

Un ejemplo lo tenemos en el ataque que se lanzó contra *Ashley Madison* en 2015, donde los atacantes fueron capaces de descifrar la contraseña de millones de cuentas de usuarios repartidos por todo el mundo [32]. Dado que muchas personas usan el mismo nombre de usuario y contraseña para la mayoría de sus cuentas, sólo es cuestión de tiempo que algunos atacantes empiecen a usarlas para secuestrar y acceder a cuentas y servicios de todo el planeta.

5.1.4 Interfaces y APIs de gestión inseguras (T4)

Fuente: CSA, ENISA

Impacto: Confidencialidad, autenticación, integridad

Los proveedores de almacenamiento en la nube exponen y proporcionan un conjunto de **interfaces y API** para que sus clientes puedan gestionar e interactuar con sus servicios y recursos [14]. En muchos casos, la seguridad y disponibilidad del servicio depende de su seguridad y de cómo se usan para implementar soluciones a medida. Una mala implementación puede exponer un conjunto de vulnerabilidades, las cuales pondrán en riesgo los datos almacenados por los diferentes clientes del servicio, dado que muchos procesos de seguridad (autenticación, control de acceso, cifrado, etc.) se realizan a través de éstas. Por tanto, es importante que este conjunto de herramientas e interfaces se diseñen de forma segura, para minimizar los riesgos de seguridad. Ya que las API e interfaces son accesibles desde cualquier lugar en Internet, un atacante podría usarlas para comprometer la seguridad de los datos de los usuarios del servicio [22].

5.1.5 Denegación de Servicio – DoS y DDoS (T5)

Fuente: CSA, ENISA

Impacto: Disponibilidad

Un **ataque de DoS o DDoS** puede impedir a los usuarios legítimos del servicio acceder a sus datos, mediante el uso de técnicas que consumen recursos de los sistemas (procesador, memoria, espacio de disco, etc.) o del ancho de banda de la red del proveedor [22].

5.1.6 Personal interno malicioso (T6)

Fuente: CSA, ENISA

Impacto: Confidencialidad, disponibilidad, integridad

El **personal interno malicioso** de una organización puede definirse como un empleado, exempleado, contratista u otro socio comercial, que tiene o ha tenido autorización para acceder a la red, los sistemas o los datos de una organización e intencionadamente abusa de sus privilegios de acceso, afectando negativamente a la confidencialidad, integridad o disponibilidad de la información [22]. A este respecto, un estudio realizado por Symantec en 2013 concluye que aproximadamente la mitad de los empleados que perdieron sus puestos de trabajo o los dejaron voluntariamente mantuvo en su poder datos corporativos confidenciales y un 40% pensaba usarlos en sus nuevas empresas [28], lo que significa que una parte de la propiedad intelectual de las organizaciones cae en manos de sus competidores.

Uno de los ejemplos más conocidos de personal interno malicioso para una organización es el caso *Snowden* [61]. Antiguo trabajador de la *Central Intelligence Agency* (CIA) y la *National Security Agency* (NSA), en 2013 filtró documentos confidenciales, clasificados como de alto secreto por las autoridades estadounidenses, a importantes publicaciones anglosajonas.

5.1.7 Fallos en la tecnología de compartición - fallo de aislamiento (T7)

Fuente: CSA, ENISA

Impacto: Confidencialidad, disponibilidad, integridad

Cualquier vulnerabilidad en los diferentes sistemas que gestionan la **compartición de tecnología** en la nube, como puede ser el *hypervisor*, puede significar una violación o pérdida de los datos almacenados de sus usuarios, además de comprometer al sistema *cloud* por completo [22] [24]. Por ejemplo, en 2012 un fallo en el *hypervisor* en la plataforma *Xen*, permitió a los atacantes obtener derechos de administración del sistema y así ejecutar código arbitrario o acceder a cualquier cuenta de usuario y sus datos [33].

5.1.8 Software vulnerable (T8)

Fuente: ENISA

Impacto: Confidencialidad, autenticación, disponibilidad, integridad

En la nube, cualquier **vulnerabilidad en el software** puede suponer un gran impacto para la información almacenada en sus sistemas. Por ejemplo, si un proveedor ofrece un cliente para el acceso a su servicio de almacenamiento vulnerable a *Cross-Site Scripting* o *SQL Injection*, un ataque podría provocar una violación de los datos de sus usuarios. Un ejemplo de vulnerabilidad en el software la proporciona una actualización del cliente de Dropbox en 2011, la cual aparentemente permitía acceder a una cuenta de Dropbox sin la necesidad de introducir una contraseña válida, lo que hacía posible que cualquiera pudiera entrar en la cuenta de otros usuarios y comprometer así sus datos almacenados [34].

5.1.9 Cumplimiento de la legislación vigente (T9)

Fuente: ENISA

Impacto: Confidencialidad, integridad

Los **usuarios**, en última instancia, **son responsables** de la seguridad e integridad de sus datos, aunque se encuentren gestionados por un proveedor de almacenamiento en la nube [14], siendo por tanto responsables del cumplimiento de la legislación aplicable en materia de protección de datos. En el caso de España, aplican la Ley Orgánica de Protección de Datos (LOPD) y la directiva europea 95/46/CE sobre **protección de datos personales** [42], entre otras leyes. Debe tenerse en cuenta que el proveedor del servicio puede tener sus centros de datos repartidos por diferentes países, con lo que la **jurisdicción** de cada uno podrá tener un impacto significativo a nivel de seguridad y privacidad de los datos [25]. Por ejemplo, en el caso de que un juez estadounidense dictamine requisar un disco duro con datos personales para su inspección, perteneciente a un centro de datos de un proveedor de almacenamiento en la nube, ¿qué ocurre si contiene datos personales recogidos en España y protegidos por la LOPD? Existen tratados internacionales para estos casos, como el Marco de Puerto Seguro entre la UE y EE.UU., que fue invalidado el 6 de octubre de 2015 por la Corte Europea de Justicia [27], amenazando con que las transmisiones de datos personales a proveedores localizados en EE.UU. puedan ser suspendidas en España y el resto de la UE en un futuro [42].

5.1.10 Ataques a la red (T10)

Fuente: ENISA

Impacto: Confidencialidad, disponibilidad, integridad

Puesto que los servicios de almacenamiento en la nube se consumen a través de Internet, existe un **riesgo importante de sufrir diferentes tipos de ataques**, como pueden ser, entre otros, el análisis de tráfico de red, *eavesdroping*, *spoofing*, modificación de datos en tránsito, *pharming, man-in-the-middle*, etc. [25].

5.1.11 Robo o pérdida de dispositivos (T11)

Fuente: ENISA

Impacto: Confidencialidad, autenticación, disponibilidad, integridad

Hoy día una gran mayoría de nosotros llevamos un **dispositivo móvil** en el bolsillo con un cliente de almacenamiento en la nube instalado (Google Drive, OneDrive, CloudMe, Yandex.Disk, etc.). El dispositivo puede contener certificados digitales, gestores de claves, etc., que aseguran el acceso a diferentes tipos de aplicaciones y servicios, entre ellos a los clientes de almacenamiento, que suelen estar conectados constantemente y en sincronización. Si cae en malas manos, significa que tanto las credenciales como los datos pueden ser robados por un atacante: accediendo directamente a través de los clientes del servicio, obteniendo las credenciales para posteriormente entrar a la cuenta, etc.

Un ejemplo de robo con consecuencias para la privacidad de los datos ocurrió en 2014, cuando fue robado de su vehículo el ordenador de un empleado del centro *Northwestern Memorial HealthCare* de EE.UU., que contenía datos confidenciales de casi tres mil usuarios y pacientes [35].

5.2 Aspectos de seguridad del almacenamiento en la nube

El apartado anterior introdujo algunas de las principales amenazas de seguridad contra las que se enfrenta el almacenamiento en la nube. En éste, se describen algunos aspectos relevantes a tener en cuenta para su seguridad, dando como resultado una serie de requisitos destinados a mitigar el impacto de las amenazas sobre los datos de los usuarios, en términos de su confidencialidad, autenticación, integridad y disponibilidad. Estos aspectos son [17] [18]:

- Seguridad del transporte.
- Registro y login de usuario.
- Disponibilidad, confidencialidad e integridad de datos en el proveedor.
- Compartición y acceso de datos.

- Deduplicación de datos.
- Múltiples dispositivos.
- Borrado de datos.
- Actualizaciones del software cliente.
- Localización de los servidores de almacenamiento.
- Legislación.

En los siguientes subapartados puede verse una descripción de cada uno de estos aspectos y los requisitos de seguridad que de ellos se derivan.

5.2.1 Seguridad del transporte (A1)

En los servicios en la nube, todas **las comunicaciones se realizan a través de la red**, tanto las que se llevan a cabo entre las aplicaciones cliente y el proveedor del servicio como entre los sistemas de almacenamiento del propio proveedor: registro de nuevos usuarios, autenticación, copia y descarga de archivos, sincronización entre dispositivos y entre los nodos del proveedor, etc. Esto provoca que las comunicaciones de los servicios en la nube puedan ser **objeto de ataques** (amenaza T10) para conseguir, por ejemplo, el robo de credenciales de los usuarios (amenaza T3) y obtener o manipular el contenido de la información que se está transmitiendo (amenaza T1).

Para **mitigar el impacto** sobre los datos de los usuarios, que tienen los ataques contra el transporte de la información, será necesario asegurar las comunicaciones en términos de autenticidad, confidencialidad e integridad. Por tanto, de aquí pueden extraerse **algunos** de los **requisitos** de seguridad para el transporte de datos de los servicios de almacenamiento [17] [18]:

- **Confidencialidad e integridad de las comunicaciones** mediante el uso de sistemas y protocolos criptográficos modernos y contrastados, como TLS en lugar de SSL [36].
- **Autenticación del servidor** mediante el uso de certificados digitales emitidos por autoridades de confianza, que permitan a las aplicaciones cliente verificar que realmente está conectado con el proveedor de servicio correcto, permitiendo mitigar, entre otros, ataques *man-in-the-middle* o *phishing* [36].

5.2.2 Registro y login de usuario (A2)

Para que un usuario pueda trabajar con cualquier servicio de almacenamiento en la nube, se requiere que éste complete un primer **proceso de registro** en los sistemas del proveedor. En los servicios gratuitos, normalmente suele ser suficiente con crear una cuenta de usuario, en la que se proporciona un mínimo de información. En los de pago, la información a suministrar es bastante más amplia y comprometida (cuenta bancaria, tarjeta de crédito, domicilio, datos fiscales, etc.). Una vez registrado, el usuario debe realizar un **login**, desde las aplicaciones cliente que utilice, para poder trabajar con los servicios proporcionados por su proveedor. Toda esta información se envía a través de la red al proveedor, por lo que deben estar aseguradas las comunicaciones en el sentido apuntado en el aspecto A1.

La importancia de estos procesos, **registro y login**, por la información que transmiten (credenciales de los usuarios del servicio), hace que sean susceptibles de ser atacados para, entre otros, intentar acceder al servicio en nombre de un usuario legítimo (amenaza T3) y así acceder a sus datos (amenaza T1) o denegarle el acceso (amenaza T5) mediante la modificación de sus credenciales. Dicho esto, algunos de los **requisitos** de seguridad para el registro y login del usuario en un servicio de almacenamiento en la nube deberían ser los siguientes [17] [18]:

- **Autenticación del usuario** hacia el proveedor del servicio, normalmente mediante el uso de usuario y contraseña.
- **Uso de contraseñas robustas**. El proveedor debería solicitar el uso de contraseñas robustas a sus usuarios y rechazar las que no cumplan con los criterios establecidos. OWASP [48]

sugiere una serie de características que debería cumplir una contraseña para ser considerada robusta, como pueden ser, entre otras: longitud mínima de 10 caracteres de diferentes tipos (letras, números y caracteres especiales), no contener más de dos caracteres iguales seguidos, información personal del usuario ni palabras claves como *"password"*.

- **Autenticación multifactor**. Aunque podría considerarse como un requisito opcional, es aconsejable que los proveedores permitan la autenticación multifactor y que los usuarios la utilicen, añadiendo más protección durante el proceso de autenticación del usuario [10].
- **Minimización de la recolección de datos**. Sería conveniente que, en la fase de registro de usuarios, se limitase la información necesaria a recopilar para operar correctamente el servicio, con el objetivo de mitigar un potencial robo de información. Por ejemplo, si el servicio no es de pago, solicitar el DNI o el número de tarjeta de crédito no sería apropiado.
- **Solicitud activación cuenta**. Antes de poder usar una cuenta nueva, el proveedor del servicio debería solicitar su activación al usuario que se registre. Existen diferentes métodos, como el envío de un código de activación por SMS o un correo electrónico con un enlace para activar la cuenta.
- **Solicitud de una nueva contraseña** durante la activación de la cuenta. En el mismo proceso de activación, sobre todo si la contraseña no la eligió el propio usuario durante el registro, el proveedor debe solicitarle al usuario que la modifique e introduzca una nueva.
- **Protección contra enumeración de usuarios**. Un ataque de enumeración de usuario permitiría obtener listas de cuentas de usuario existentes, del servicio de almacenamiento en la nube, desde las páginas de registro, login y recuerdo de contraseñas [37].

5.2.3 Disponibilidad, confidencialidad e integridad de datos en el proveedor (A3)

Uno de los propósitos del almacenamiento en la nube es permitir a sus usuarios tener copias de sus datos fuera de sus instalaciones y que sean de fácil acceso. Normalmente, estos datos son valiosos para sus propietarios (estrategias de negocio, pólizas de seguros, fotos comprometidas, etc.), que confían a su proveedor para mantenerlos protegidos ante posibles amenazas, como las del apartado 5.1, la cuales pueden significar su **violación** o **pérdida** definitiva.

Para **mitigar el impacto** de los posibles ataques contra los datos en las instalaciones del proveedor, deberían tenerse en cuenta, entre otros, los siguientes requisitos de seguridad [16] [17]:

- **Cifrado de datos en el lado cliente** (*encrypt yourself*). Asegura la información tanto en tránsito como en las instalaciones del proveedor, impidiendo que el propio proveedor tenga acceso a su contenido. En este caso, las claves de cifrado deberían estar controladas por los propios usuarios y ser desconocidas por el proveedor.
- Establecer mecanismos de **control de acceso a los datos** de los usuarios en el proveedor. Es decir, mecanismos que controlan los accesos de los usuarios, definición de privilegios de acceso, trazas de actividad, etc.
- El proveedor debería definir una política de ***backups*** y **replicación** de datos almacenados en sus instalaciones.
- Uso de **sistemas antivirus** actualizados y contrastados, que garanticen que los archivos que almacenen los usuarios estén libres de *malware*.
- El proveedor debería definir un **plan de desastres**, describiendo qué acciones se llevarán a cabo, por ejemplo, ante el fallo de discos y servidores o el incendio de una instalación.

5.2.4 Compartición y acceso de datos (A4)

La **compartición de los datos almacenados** en la nube es uno de los principales requisitos existentes en la actualidad, tanto para usuarios particulares (fotos de familia, prácticas del colegio, listas de nombres, documentos de identidad, teléfonos, direcciones de correo, etc.) como para organizaciones que buscan mejorar su productividad y beneficios (compartición de documentos de trabajo, datos de los pacientes de un hospital, listas confidenciales de personas incluidas en un ERE, etc.). En general, podría decirse que a la gente le gusta compartir información por muy diferentes

motivos, aportándoles una serie de beneficios: mayor productividad, disfrute personal, compartir opiniones, darse a conocer en el mercado laboral, etc. [26].

Sin embargo, la compartición de información en la nube pone en **riesgo la seguridad y privacidad de los datos** de sus usuarios. Por ejemplo, en la compartición a través de enlaces (usado por muchos proveedores de almacenamiento en la nube), cualquier persona que tenga acceso a un enlace, o pueda predecirlo de alguna forma, puede tener acceso a su información, a no ser que ésta esté cifrada. Según un estudio llevado a cabo por la *Enterprise Management Associates* (EMA) en 2015 [29], el 83% de las organizaciones consultadas indicaron que se habían producido fugas o pérdidas de información debido al mal uso de la compartición o al acceso no autorizado a los datos.

Para mitigar las **amenazas** ocasionadas por la **compartición de información en la nube**, como podría ser la de violación de datos (T1), se requiere de la implementación, por parte de los proveedores del servicio, de métodos fiables de control de acceso a los datos, como ya se indicó en el aspecto A3, además de la correcta aplicación por parte de sus usuarios. Por otro lado, aunque el cifrado de los datos almacenados también es aconsejable, se presenta el problema de la compartición de las claves de cifrado entre los diferentes actores con acceso a los datos [26]. Por tanto, visto esto, los requisitos de seguridad para la compartición y acceso de datos, entre otros, podrían ser los siguientes [17] [26]:

- **Confidencialidad de los datos**. Sólo quien tenga autorización, podrá tener acceso a los datos almacenados y compartidos por los usuarios del servicio en la nube.
- La **autorización de acceso** a otros usuarios, deberá ser concedida y revocada sólo por el propietario de los datos, que es el único que puede especificar quién tiene **permisos** de lectura, escritura o borrado de los datos compartidos.
- Los datos **no** deberán ser **indexados** por ningún motor de búsqueda, sin el consentimiento de su propietario.
- El propietario de los datos ha de poder acceder a un **listado de la información** que tiene **compartida** en cada momento.
- El proveedor del servicio debe indicar claramente el **método de compartición** que provee.

5.2.5 Deduplicación de datos (A5)

La técnica de **deduplicación de datos** es usada por los proveedores para poder ahorrar espacio de almacenamiento, eliminando redundancias cuando se reciben dos o más copias de los mismos datos. Existen diferentes alternativas de deduplicación (una explicación resumida de las cuales puede encontrarse en el Anexo A):

- Deduplicación en cliente o deduplicación en el servidor.
- Deduplicación *single-user* o deduplicación *cross-user*.
- Deduplicación a nivel de archivo o deduplicación a nivel de bloque.

Esta técnica no está exenta de **amenazas a la privacidad** de los datos almacenados, por ejemplo, si se usa al mismo tiempo la deduplicación en cliente y *cross-user*, un atacante podría averiguar qué archivos están almacenados en el proveedor del servicio y obtener información sobre un usuario específico. Por tanto, una propuesta de requisito de seguridad sería que el proveedor no use la combinación *cliente – cross-user* [17]

5.2.6 Múltiples dispositivos (A6)

Hoy día existen **multitud de dispositivos** que permiten trabajar con servicios de almacenamiento en la nube. Todos los usuarios tenemos normalmente más de uno, como pueden ser: los ordenadores de casa y del trabajo, uno o varios *smartphones*, tabletas, libros electrónicos o televisiones inteligentes.

Uno de los requisitos de los usuarios con más de un dispositivo es que sus datos estén permanentemente **sincronizados** entre todos ellos, lo que implica que la misma cuenta de usuario deba estar asociada con cada uno de estos dispositivos. Esto último implica que el usuario, cuando instala un nuevo cliente en un dispositivo, tendrá que proporcionar sus **credenciales** para asociarlo a su cuenta, las cuales serán almacenadas en local para no tener que ser introducidas a cada momento. En estos casos, existe el riesgo de que un atacante sea capaz de conseguir las credenciales de un usuario (amenaza T3) conectado con un dispositivo móvil, por ejemplo, a una red WiFi abierta (amenaza T10). Una vez obtenidas estas credenciales, estará en disposición de poder **violar la cuenta y datos** de su usuario (amenaza T1). Además, si un dispositivo cae en malas manos (amenaza T11) y no está convenientemente protegido, el atacante podría tener acceso a sus datos, tanto los almacenados en la nube a través de la aplicación cliente instalada en el dispositivo como los descargados en el dispositivo. Por tanto, a parte de los propios requisitos de protección del dispositivo, los proveedores del servicio deberían proporcionar la siguiente funcionalidad para gestionar los dispositivos asociados a un usuario [17]:

- Mantener un **listado de los dispositivos** registrados para un mismo usuario.
- **Activación y desactivación** de un dispositivo manualmente por parte sus propietarios.
- El usuario ha de poder **seleccionar el nombre** de sus dispositivos.

5.2.7 Borrado de datos (A7)

El comportamiento ante el **borrado de datos** puede variar entre diferentes proveedores de almacenamiento en la nube, aunque es común el mantenimiento de los datos durante un determinado periodo de tiempo y antes de borrarlos definitivamente [18]. Una eliminación inadecuada de los datos puede ocasionar una **violación** de los mismos por parte de un atacante. Por tanto, los requisitos de seguridad para la compartición y acceso de datos, entre otros, deberían ser los siguientes [16]:

- Los datos borrados han de ser completamente **eliminados de todos los sistemas** del proveedor del servicio, incluso de las copias de *backup* que pudieran existir.
- La eliminación de la información debe **sincronizarse** con todos los dispositivos del usuario.
- El **espacio** que ocupan los datos borrados debe ser **sobrescrito** para asegurar que no son recuperados.
- No debe existir un **periodo de retención** de los datos sin el consentimiento del usuario.

5.2.8 Actualizaciones del software cliente (A8)

Ejecutar versiones antiguas de una aplicación cliente implica estar expuestos a una serie de riesgos de seguridad (amenaza T8), puesto que puede contener vulnerabilidades que han sido resueltas en una versión más moderna [17]. Para mitigar este problema, sería conveniente el cumplimiento, entre otros, de los siguientes requisitos en las aplicaciones cliente del almacenamiento en la nube [17]:

- **Chequeo regular y automático** de la actualización del software de cliente.
- El inicio de las **actualizaciones** han de poder ser **automáticas** o a **instancias del usuario**.
- Llevar un **registro** detallado **de** los **cambios** realizados.

5.2.9 Localización de los servidores de almacenamiento (A9)

Al utilizar el servicio de almacenamiento en la nube, no siempre se conoce de forma exacta en qué país pueden estar **localizados los datos almacenados** [14]. Este hecho, puede suponer una amenaza para el cumplimiento de las diferentes legislaciones, tal y como se vio en el apartado 5.1. Por tanto, es necesario que:

- El proveedor del servicio proporcione **información sobre la localización** de sus centros de datos, en los que almacenará la información de sus usuarios y *backups*.
- El cliente pueda **seleccionar la localización** para almacenar sus datos.

5.2.10 Legislación (A10)

Como se introdujo al hablar del cumplimiento de la legislación vigente en el apartado 5.1 (amenaza T9), los usuarios son responsables en última instancia de la seguridad e integridad de sus datos. Existen una serie de **leyes nacionales** de cada país y **tratados internacionales** que deben considerarse a la hora de seleccionar un proveedor de almacenamiento en la nube. Por ejemplo, un usuario localizado en España, que quiera almacenar datos de carácter personal, debería considerar el cumplimiento de [42]:

- La **LOPD** 15/1999, de 13 de diciembre de 1999.
- La directiva europea **95/46/EC**, de 24 de octubre de 1995.
- Los **requisitos** para poder **exportar** datos personales fuera de España y la UE.
- Los **tratados internacionales** con países terceros.

- Página dejada en blanco intencionadamente -

6. Análisis de seguridad de productos de almacenamiento

Con el objetivo de conocer la seguridad de un producto de almacenamiento en la nube, es necesario realizar primero un análisis que permita a sus potenciales usuarios decidir si cumple con sus requisitos de seguridad. El análisis debería completarse con una comparación de resultados para otros productos y así disponer de información suficiente para tomar una decisión sobre el producto que se adapta mejor a las necesidades especificadas.

En este capítulo, se realizará el análisis de tres productos que ofrecen almacenamiento en la nube de forma gratuita: Yandex.Disk, CloudMe y Google Drive. Para su análisis, se estudiarán los procesos comunes para todos los productos, dando como resultado si cumplen o no con los requisitos de seguridad seleccionados.

6.1 Productos a analizar

Hoy día, existen muchos proveedores que proporcionan productos de almacenamiento en la nube, tanto gratuitos como de pago. Normalmente, el uso gratuito del servicio está restringido a un periodo de tiempo o límite de almacenamiento; el sobrepasarlos implica el abono de una tarifa por su uso. Estudiar la seguridad de todos los productos es una tarea ingente que está fuera del alcance de este trabajo, por lo que se han escogido tres de estos productos, que ofrecen servicios gratuitos y de pago: Yandex.Disk, Google Drive y CloudMe.

La razón principal para la elección de Yandex.Disk, servicio prestado por el mayor proveedor de Internet ruso, ha sido la de conocer la seguridad que ofrece un producto ubicado en Rusia, cuyo proveedor intenta expandirse hacia el oeste europeo, con el fin de competir con otros productos en la nube, que son principalmente norteamericanos.

La elección de Google Drive, proveído por el gigante mundial de Internet Google, se debe a su gran popularidad entre los usuarios europeos y a su diseño, al igual que Yandex.Disk, para trabajar con aplicaciones cliente de forma *standalone* en multitud de dispositivos. Aunque es un producto estadounidense, tiene localizaciones por todo el planeta. Una de las principales preocupaciones, al trabajar con este producto, es la legislación y jurisdicción aplicables, teniendo en cuenta que el marco de trabajo *Safe Harbor* firmado entre EE.UU. y la UE ha sido derogado por los tribunales europeos.

En cuanto a CloudMe se ha escogido por ser un proveedor de almacenamiento en la nube ubicado dentro de la UE, concretamente en Suecia, y por tanto se encuentra dentro de su marco legislativo, que es completamente compatible con la legislación española.

6.2 Metodología de Análisis

Todo análisis necesita establecer primero unas pautas de trabajo, es decir un marco desde el cual realizar nuestra tarea: analizar la seguridad de diferentes productos de almacenamiento en la nube. En el presente trabajo, se han tenido en cuenta las metodologías propuestas por [17] y [18] para realizar el análisis de los productos de almacenamiento en la nube seleccionados. Por tanto, las tareas y pasos necesarios para llevar a término el trabajo propuesto pueden resumirse en:

1. **Seleccionar requisitos** de seguridad, en base a los aspectos y amenazas estudiados en capítulos anteriores.
2. **Seleccionar los procesos** de los productos que quieren analizarse. Por ejemplo: conexión, transmisión de datos, borrado, etc. A cada proceso se le asignarán los requisitos que deben cumplir.

3. **Analizar la seguridad de los procesos**. Su resultado debe ser si cumplen o no con los requisitos, siempre y cuando exista información suficiente para determinarlo.
4. **Comparar** los resultados entre los productos.

6.3 Requisitos de seguridad y privacidad

Para poder llevar a cabo el análisis de los productos seleccionados, debe obtenerse primero un conjunto de requisitos como base para su realización. Algunos de estos pueden verse en el capítulo 5, donde se abordan los aspectos de seguridad, para intentar mitigar algunos de los posibles ataques al almacenamiento en la nube. En la Tabla 4 se listan los que se tendrán en cuenta para este trabajo.

Id	Requisitos de seguridad y privacidad
R1	Confidencialidad e integridad de las comunicaciones entre las aplicaciones cliente y el proveedor del almacenamiento en la nube, usando protocolos de seguridad y criptografía adecuados.
R2	Uso de contraseñas robustas, rechazando las que no cumplen unos criterios mínimos, según las características definidas por OWASP en [48].
R3	Autenticación del servidor contra una aplicación cliente que inicie cualquier comunicación.
R4	Autenticación de los clientes al acceder al almacenamiento en la nube, como mínimo mediante el uso de nombre de usuario y contraseña.
R5	Los proveedores deben proporcionar la posibilidad de usar la autenticación multifactor.
R6	Minimización de la recolección de datos durante el registro de un usuario nuevo en el servicio.
R7	Solicitud de la activación de la cuenta de usuario, después de haber finalizado el registro en el servicio. Si el usuario no había escogido la contraseña, en el mismo proceso de activación deberá solicitársele al usuario que cree su propia contraseña.
R8	Protección contra enumeración de usuario, durante las etapas de registro y *login* de usuario.
R9	Cifrado de datos en el lado cliente (*encrypt yourself*), usando criptografía adecuada y moderna.
R10	Sólo quién tenga autorización podrá tener acceso a los datos de un usuario. La autorización de acceso a los datos compartidos debe ser concedida y revocada sólo por su propietario, siendo el único que puede especificar quién tiene permisos de lectura/escritura.
R11	Sin el consentimiento de su propietario, en ningún caso los datos almacenados en la nube deben ser indexados por motores de búsqueda.
R12	Un usuario ha de poder acceder a un listado con los datos que tiene compartidos en la actualidad con otros usuarios.
R14	El proveedor del servicio debe indicar claramente el método de compartición que provee.
R15	El proveedor del producto no debería implementar la deduplicación con la combinación *cliente – cross-user*, puesto que no está excepta de vulnerabilidades [17].
R16	El proveedor debe mantener un listado actualizado de los dispositivos registrados, en los que un usuario tiene alguna de sus aplicaciones cliente instaladas.
R17	La activación y desactivación de un dispositivo debe hacerse manualmente por parte del usuario del servicio.
R18	El usuario ha de poder seleccionar el nombre de sus dispositivos.
R19	Los datos borrados deberían ser completamente eliminados de todos los sistemas y sincronizarse con todos los dispositivos que tengan acceso.
R20	El espacio que ocupan los datos borrados debe ser sobrescrito para asegurar que no son recuperados.
R21	No debería existir en ningún caso un periodo de retención de los datos antes de eliminarse definitivamente.
R22	Chequeo regular y automático de la actualización del software de cliente. El inicio de las actualizaciones ha de poder ser automático o a instancias del usuario.
R23	Debería existir un registro detallado de los cambios realizados en el software del cliente durante su actualización.
R24	El proveedor debe proporcionar información sobre la localización de los datos y sus *backups*.
R25	El usuario ha de poder seleccionar la localización de sus datos en la nube, principalmente para cumplir con la legislación al que está sujeto.

Id	Requisitos de seguridad y privacidad
R26	Cumplimiento en España de la LOPD, la directiva europea 95/46/EC de 1995 sobre protección de datos, tratados con países terceros, requisitos de exportación de datos personales fuera de la UE [42] y otras leyes a las que pueda estar sujeto un usuario.
R27	El proveedor del almacenamiento en la nube debe realizar un *backup* regular de los datos que sus usuarios tienen almacenados en sus instalaciones.
R28	El proveedor debe garantizar la integridad de los archivos que se transmiten entre sus clientes y proveedores. Es decir, debe garantizar que el archivo que se envía y el que se recibe en el otro lado no ha sido modificado, independientemente del protocolo de comunicaciones.
R29	El proveedor debe garantizar la protección contra *malware* en el almacenamiento que sirve.
R30	El proveedor debe garantizar la integridad de los datos almacenados por sus usuarios en sus instalaciones.

TABLA 4 - REQUISITOS DE SEGURIDAD Y PRIVACIDAD

6.4 Procesos a analizar

Tal y como se ha visto anteriormente, deben seleccionarse los procesos de los productos a analizar. En este trabajo se han dividido los procesos en tres partes:

1. Los relacionados con los protocolos de comunicaciones implementados. En concreto, se estudiarán la conexión, el proceso de registro para los nuevos usuarios y el de *login* para los usuarios ya existentes.
2. Los relacionados con el tratamiento de la información, donde se estudiarán la transmisión de datos, su almacenamiento, la compartición y el borrado. En estos casos, se tendrá en cuenta el cumplimiento de la legislación vigente en España y la UE.
3. Gestión de los dispositivos que soportan los clientes de los productos.

Cada una de los procesos, como se indicó más arriba, deben cumplir los requisitos tal y como pueden verse en la Tabla 5, con las siguientes consideraciones:

- Por **conexión** se entenderá cualquier establecimiento de comunicación entre el cliente y los servidores del proveedor, en los que se deban intercambiar datos. Incluye principalmente: registro, login y transmisión de archivos. Cualquier conexión deberá cumplir con los requisitos R1 y R3. Por esta razón, por ejemplo, no asignamos el requisito R1 al proceso de transmisión de archivos, puesto que ya se supone que debe cumplirlo por el simple hecho de tener que realizar una conexión previa.
- El requisito **R9** aplica tanto para la **transmisión de archivos** como para su **almacenamiento**. En el primer caso se quiere indica que el cliente debe cifrar los archivos antes de iniciar su subida a los servidores del proveedor, con el fin de que ningún atacante que comprometa los servidores pueda interceptarlos y revelar su información. Por otro, se requiere que el archivo debe almacenarse cifrado en las instalaciones del proveedor, pero que el cifrado debe ser realizado por el cliente, independientemente de si los servidores también los cifran, con el fin de garantizar la seguridad en el lado del proveedor.

Procesos	Requisitos
Comunicaciones	
Conexiones	R1, R3
Registro	R2, R6, R7, R8
Login	R4, R5, R8
Tratamiento de la información	
Transmisión de archivos	R9, R15, R28
Almacenamiento	R9, R10, R24, R25, R27, R29, R30
Compartición	R10, R11, R12, R14
Borrado	R19, R20, R21
Cumplimiento de la legislación	R26
Gestión de los dispositivos cliente	

Procesos	Requisitos
Gestión multidispositivo	R16, R17, R18
Actualización del software cliente	R22, R23

TABLA 5 – RELACIÓN ENTRE LOS COMPONENTES DE ANÁLISIS Y LOS REQUISITOS A ESTUDIAR

6.5 Análisis de los productos seleccionados

En los siguientes apartados se aplicará la metodología definida más arriba para analizar los productos, tomando como clientes las soluciones *standalone* que proporcionan (principalmente para entornos Windows y Linux) o *web*. Las principales herramientas usadas para el análisis serán:

- Documentación proporcionada por los proveedores.
- *Wireshark* y ZAP de OWASP, junto con el *plugin* para Firefox, para analizar el tráfico generado por los diferentes clientes.
- Archivos de trazas de los clientes de los productos.

6.5.1 Yandex.Disk

Yandesk.Disk (https://disk.yandex.com/) es un producto de almacenamiento en la nube que viene de la mano del principal proveedor ruso Yandex.ru, llamado a menudo el "Google ruso". Yandex es la compañía de servicios en la nube más extendida en Rusia, Turquía y otros países de su entorno [44]. Actualmente está intentando su expansión al resto del continente europeo y EE.UU., para competir con otros productos ya consolidados, como Google Drive o Dropbox [45].

Yandex.Disk ofrece almacenamiento gratuito en la nube con capacidad de 10GB por cuenta, aunque puede ampliarse gratuitamente hasta 20GB mediante invitaciones a amigos y otras promociones que van publicando. Existe la posibilidad de comprar almacenamiento extra de 10GB a 10$ anuales, 100GB a 50$ anuales o 1TB a 300$ anuales [38].

Según su documentación, permite gestionar los archivos de sus usuarios desde aplicaciones clientes instaladas en diferentes dispositivos conectados a Internet:

- Ordenadores personales con Microsoft Windows, Linux o Mac OS X.
- Dispositivos móviles con Android, iOS, Symbian o Windows Phone.

Yandex.Disk soporta los protocolos WebDAV y RESTful, proporcionando las API para poder implementar aplicaciones clientes que interactúen con el servicio de almacenamiento en la nube. Puesto que soporta el protocolo WebDAV, hace posible a un usuario conectarse desde su sistema operativo a su almacenamiento en la nube como si fuera una unidad de red más, sin la necesidad de instalar ningún tipo de cliente [38].

En este estudio, se analizará el cumplimiento de los requisitos para la consola *web* y los clientes de Windows y Linux, principalmente por una cuestión de extensión y acotación del trabajo en el tiempo.

Ofrece diversas desventajas que pueden hacer dudar a la hora de escogerlo como almacenamiento para nuestra información en la nube:

- La mayoría de documentación está en ruso, aunque cada vez más puede accederse a su traducción en inglés.
- El hecho de que la Agencia Española de Protección de Datos (AEPD) no incluya a Rusia como país con un nivel adecuado de protección, hace que no sea un servicio de almacenamiento

en la nube demasiado adecuado para almacenar archivos con información protegida por la LOPD y otras leyes en materia de protección de datos de la Unión Europea.

6.5.1.1 Comunicaciones

6.5.1.1.1 Conexión

En las pruebas realizadas, para **asegurar** las **comunicaciones** entre los clientes y sus servidores, Yandex.Disk usa el protocolo seguro TLS, versión 1.2. En todas las comunicaciones, los servidores han escogido la **suite de cifrado** TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, como en la Figura 2, aunque los clientes han presentado las que pueden verse en la Figura 2, durante el proceso de negociación de claves. Sus principales características pueden verse en el Anexo A. Puede decirse, por tanto, que cumple con el requisito **R1** al proporcionar **confidencialidad** e **integridad en las comunicaciones** (en la Figura 4 se muestra una captura de tráfico cifrado entre el cliente Windows de Yandex.Disk y su servidor).

En cuanto a la autenticación de los servidores, estos utilizan un certificado digital con clave pública RSA y firmado por una autoridad de certificación reconocida para **autenticarse ante los clientes**, como el que puede verse en la Figura 5. Por tanto, cumple con el requisito **R3**.

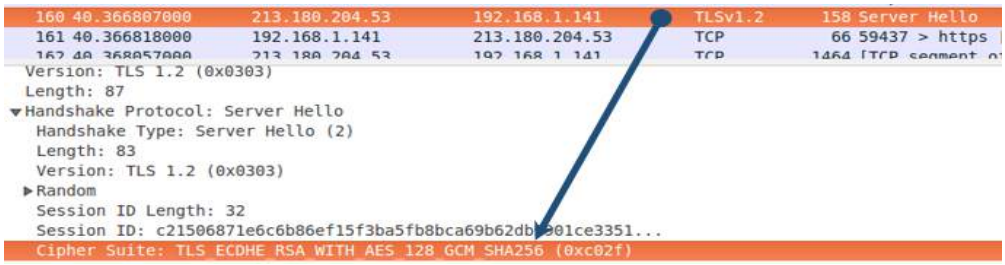


FIGURA 2 – SUITE DE CIFRADO ESTABLECIDA EN LA CONEXIÓN TLS

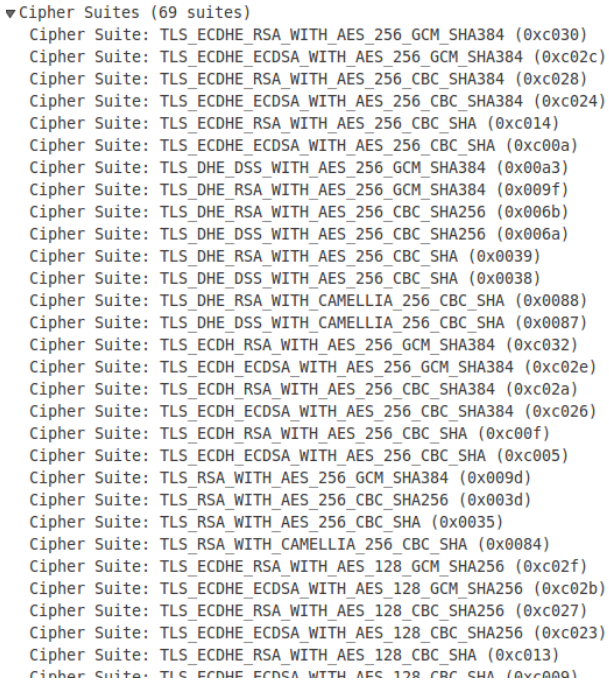


FIGURA 3 – ALGUNAS SUITES DE CIFRADO OFRECIDAS POR LOS CLIENTES EN LA CONEXIÓN TLS

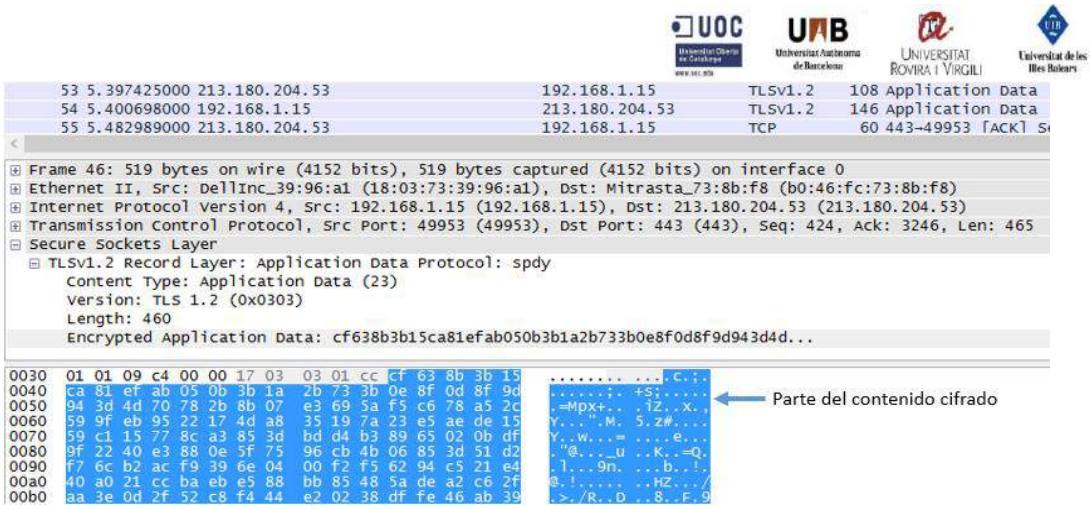


FIGURA 4 - TRANSMISIÓN CIFRADA DE ARCHIVOS DESDE EL CLIENTE WINDOWS CON TLS 1.2

FIGURA 5 - CAPTURA DEL CERTIFICADO EN LA CONEXIÓN DEL CLIENTE WINDOWS

6.5.1.1.2 Registro

Para **crear una cuenta** en Yandex.Disk, es necesario introducir la siguiente información desde su página *web*: nombre, apellido, nombre de usuario, contraseña, repetición de contraseña, número de móvil o, si no se desea introducir el móvil, una pregunta de recordatorio y un *captcha*. La **recolección de datos** parece bastante escueta, por lo que cumple con el requisito **R6**. Si el usuario ha introducido un número de móvil, Yandex.Disk le envía un código de **confirmación**, que debe introducir en el mismo formulario antes de concluir el registro. Al finalizar, si no se ha incluido el móvil, no se solicita la **confirmación** de la cuenta creada, con lo que podría decirse que el requisito **R7** se cumple sólo en parte y depende de una elección del usuario.

Debe destacarse que la **contraseña**, a pesar de enviarse a través de una conexión segura TLS, es recibida por los servidores de Yandex.Disk sin procesar por una función *hash* o similar, con lo cual estos servidores tendrán acceso a la contraseña en claro [18]. Por tanto, el personal interno o un atacante, que comprometiera la seguridad de sus servidores, podrían obtener las contraseñas de nuevos usuarios, independientemente de que posteriormente sean cifradas para almacenarlas en los

servidores. En la Figura 6 se muestra la captura con ZAP (usado como *proxy* para poder descifrar la información enviada) de una petición de registro en la cual puede observarse el envío de la contraseña sin procesar.

El formulario de registro permite la **enumeración de usuarios** existentes. La elección del nombre de usuario durante el registro da pistas sobre qué nombres pueden escogerse. Si se elige uno existente, el formulario alerta de que ya se encuentra dado de alta. Aunque sea laborioso, un atacante podría realizar una lista de usuarios de Yandex.Disk, de la forma que se muestra en la Figura 7, para lanzar un ataque posterior contra sus cuentas. Por tanto, puede concluirse que no cumple con el requisito **R8**.

FIGURA 6 - CAPTURA DE LA PETICIÓN DE REGISTRO EN YANDEX.DISK CON ZAP

FIGURA 7 - CAPTURA DE REGISTRO CON ENUMERACIÓN DE USUARIOS EN YANDEX.DISK

La **contraseña escogida** debe tener una longitud de entre 6 y 255 caracteres, y mediante pruebas, se ha podido comprobar que sólo admite caracteres del código US-ASCII. Durante la creación de la contraseña, el formulario va informando sobre su calidad y si se admite o no como válida. Solicita siempre la confirmación de la contraseña introducida. Aunque intenta fomentar el uso de contraseñas robustas, no cumple con algunas de las características propuestas por OWASP en [48], destacando la posibilidad de crear contraseñas con longitud menor de 10 caracteres. Por tanto, puede concluirse que no cumple con el requisito **R2**.

6.5.1.1.3 Login

La **autenticación básica** es de tipo usuario y contraseña para la consola *web.* En los clientes de Windows y Linux se crea un ***token* cifrado de tipo *OAuth2*** para el usuario de la cuenta a la cual se conectan [38]. De esta forma, no es necesario introducir el nombre del usuario y contraseña cada vez que quieran conectarse, excepto la primera vez cuando se configura el cliente o cuando existe un cambio de credenciales. Puede concluirse, por tanto, que cumple con el requisito **R4**, ya que existe

autenticación por parte del usuario en todos los casos. Ejemplos de *token* en Windows y Linux serían los siguientes:

Windows:
`KOO89ED+UDwpBgZDi4d3tmLyv5vDBTh+XenUVZrzH/phKxiPMZksRY9aCbh7yzisZ3HpY3s5CJ ShGmCcMsBJNvbTp8XwtUhk`

Linux:
`75aa7a5d526c1594e450a980ed012c7e072bcdb8659af94fd2bff9d9dce40df7`

Yandex.Disk permite configurar **autenticación multifactor** o *de dos pasos* [38], desde las opciones de gestión de contraseña de la consola *web* del usuario. Después de realizar los pasos necesarios, el usuario debe descargarse la aplicación Yandex.Key en su móvil, desde donde se escanea el código QR, que aparece en la pantalla de configuración, para así establecer las semillas a usar en el cálculo de las cadenas aleatorias de caracteres. Estas cadenas servirán como contraseñas de un solo uso y se recalcularán cada 30 segundos en la aplicación móvil. A partir de aquí, existen dos alternativas para autenticarse en la consola *web* del servicio:

- El usuario introduce el nombre de usuario y, como contraseña, la cadena de caracteres aleatoria, que aparece en la aplicación móvil en ese momento. Ver ejemplo en la primera imagen de la Figura 8.
- Escanear con la aplicación Yandex.Key el código QR que aparece en la página de *login* de la consola *web*, como el que puede verse en la segunda imagen de la Figura 8. Al leer el código QR, la aplicación Yandex.Key envía el nombre de usuario y una contraseña de un solo uso a Yandex para que lo autentique [38].

En cuanto a las aplicaciones cliente de Windows y Linux, es suficiente con introducir la contraseña de un sólo uso una vez para que se cree el *token OAuth2*. Por tanto, puede concluirse que cumplen con el requisito **R5** al permitir el uso de **autenticación multifactor**.

FIGURA 8 – ALTERNATIVAS DE LA AUTENTICACIÓN MULTIFACTOR: CADENA ALEATORIA Y QR

Todas las credenciales se envían a través de una conexión segura TLS. En el caso del cliente *web*, como ocurre con el proceso de registro, la contraseña no se procesa previamente por ninguna función *hash* o similar, por lo que los servidores tendrán acceso a la contraseña en claro, con lo que un atacante que comprometa los servidores de Yandex.Disk o personal interno malicioso podrán tener acceso a las contraseñas en claro de las cuentas de sus usuarios [18]. Para los clientes Windows y Linux, no ha sido posible comprobar este extremo.

El formulario de *login* permite la **enumeración de usuarios**, del mismo modo que el de registro, con lo que se concluye que no cumple con el requisito **R8**.

6.5.1.2 Tratamiento de la información

6.5.1.2.1 Transmisión de archivos

Toda la transmisión de archivos entre los servidores de Yandex.Disk y sus clientes se realiza a través de una conexión segura TLS, con lo que la transmisión queda asegurada. Sin embargo, al analizar el **cifrado de la información transmitida**, y con las pruebas realizadas, puede concluirse que los clientes *web*, Linux y Windows no cifran nativamente los archivos antes de subirlos a sus servidores. Es decir, el personal interno o un atacante que comprometa la seguridad de los servidores de Yandex.Disk podrán acceder a la información contenida en los archivos que llegan a los servidores. La Figura 9 y Figura 10 muestran dos capturas de subida y descarga de archivos respectivamente, donde puede verse el contenido en claro de los datos transmitidos entre el cliente y el proveedor. El caso de la Figura 9, se trata de la subida de un archivo de texto al disco de la cuenta del usuario, a través de la consola *web*. El de la Figura 10, muestra la descarga desde la *web* de un archivo subido previamente con el cliente Linux. Puede deducirse, por tanto, que no se cumple el requisito **R9**. El cumplimiento del requisito **R10** está en peligro, dado que un atacante podría tener acceso a la información entrante a las instalaciones del proveedor sin tener autorización para ello.

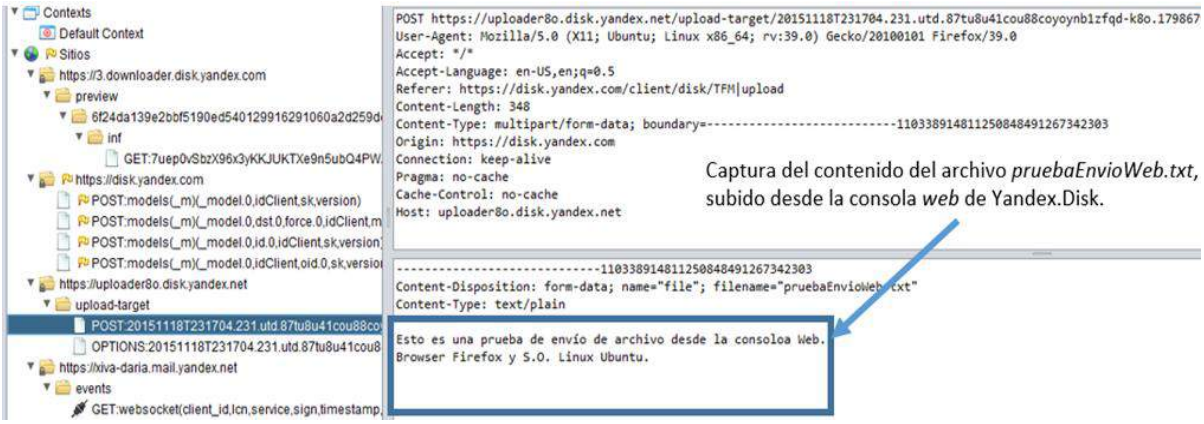


FIGURA 9 – CAPTURA CON ZAP DE LA SUBIDA DE UN ARCHIVO DE TEXTO DESDE LA CONSOLA *WEB*

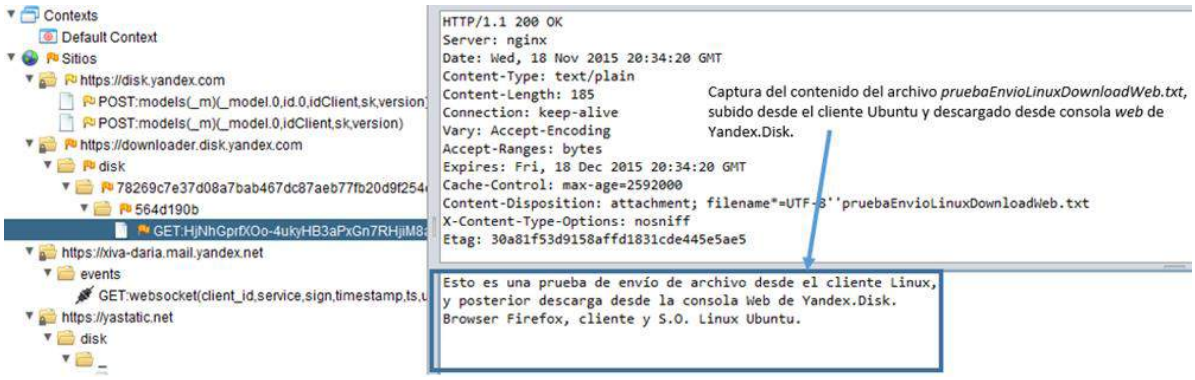


FIGURA 10 – CAPTURA DE DESCARGA DESDE LA *WEB* DE UN ARCHIVO SUBIDO CON EL CLIENTE LINUX

En cuanto al **proceso de deduplicación**, según la documentación de Yandex.Disk [38], cuando un cliente Windows o Linux quiere subir un archivo a la cuenta de su usuario, primero envía el identificador del archivo (tamaño en bytes, *checksum* MD5 – llamado *etag* – y *hash* SHA-256) al servicio de Yandex.Disk, que comprueba si ya ha sido almacenado previamente por cualquier otro usuario. Si es así, el servicio copia el archivo en la cuenta del usuario, sin necesidad de subirlo desde el dispositivo cliente, de lo contrario, se transmite completo desde el disco del cliente a sus servidores. Por tanto,

Yandex.Disk ejecuta la **deduplicación en cliente**, al ser este último el que envía la identificación del archivo para que sea comprobada por el servidor [17] [18], y **deduplicación *cross-user***, puesto que la comprobación de la existencia del archivo se realiza entre todos los usuarios de Yandex.Disk [17] [18]. Es decir, está usando la estrategia de **deduplicación "*cliente – cross-user*"**, incumpliendo así con el requisito **R15**.

Para comprobar que el funcionamiento de la deduplicación es como indica Yandex.Disk, se han realizado pruebas con tres cuentas de usuarios diferentes, con diferentes contraseñas. Llamemos a estos usuarios, X (IP 192.168.1.15), Y (IP 192.168.1.41) y Z (IP 192.168.1.141). Los dos primeros con clientes Windows y el tercero con Linux. Se genera un archivo de 200MB[1] de datos que cada uno intentará subir. Después de estudiar los ficheros de trazas de los clientes y capturas *Wireshark*, se deduce que el procedimiento es el que sigue:

1. X copia el archivo en su carpeta de Yandex.Disk. El cliente envía al servidor el identificador del archivo, ver Figura 11. El servidor, al comprobar que no existe ningún archivo con dicho identificador, le notifica al cliente de X que puede enviarlo. El cliente envía el archivo. En la Figura 12 puede verse la captura *Wireshark* con la cantidad de datos enviados por la dirección de X, columna *Bytes A ← B* de la primera línea, que se corresponden con un poco más de 200MB.
2. Y copia el mismo archivo en su carpeta de Yandex.Disk. El cliente envía al servidor el identificador del archivo. Yandex.Disk comprueba que un archivo con el mismo identificador ya ha sido almacenado, con lo que lo copia a su carpeta e indica al cliente que ya está copiado. El cliente finaliza la subida. Si el usuario accede posteriormente a su consola *web*, verá copiado el archivo en su disco. En la Figura 13 puede verse una captura de bytes transmitidos entre el servidor y el cliente de Y, donde se comprueba que la transmisión de datos es mínima.
3. Lo mismo que en el segundo caso ocurre cuando Z quiere subir la misma información a su disco de Yandex.Disk. En la Figura 14 se muestra la captura *Wireshark* (versión Linux) de los bytes transmitidos entre el cliente de Z y el servidor de Yandex.Disk.

Sin embargo, al subir un archivo desde la consola *web* del usuario, se ha podido comprobar que el servicio de Yandex.Disk no deduplica y por tanto realiza la transmisión completa de archivos, independientemente de que ya se encuentre en el disco de otro o del mismo usuario.

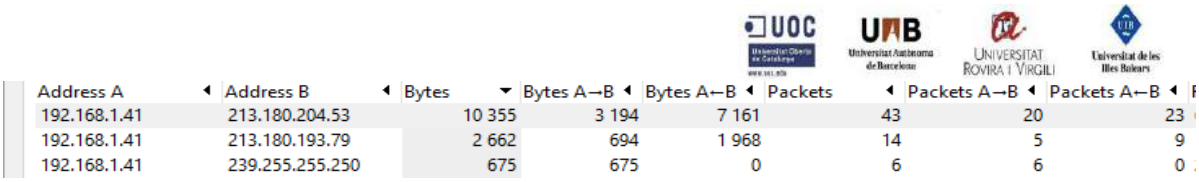

```
<iq type='set' to='[redacted]@ya.ru/YandexDisk-cli-0.1.5.940-c05650a5cf1922791983' from='[redacted]@ya.ru'>
    <query xmlns='yandex:push:disk'>
        <diff new='1448130802194286' old='1448130779688809'>
            <op key='/disk/TFM/deduplicacion.200mb'
            fid='4d691d4a8a7e1ed1def32284fbbc591f7df01ed157ba83f24312a59662aa66d5'
            md5='398ca04b4e2ed837bb97985817642e05'
            folder='/disk/TFM/'
            sha256='cf9e79241332700acda736d4a40989d6265d520259ca91b45a1ec057bb2bb747'
            type='new' resource_type='file' size='204800000'/>
        </diff>
    </query>
</iq>
```

FIGURA 11 – TRAZA DE UN CLIENTE EN LA QUE SE MUESTRA EL IDENTIFICADOR DEL ARCHIVO A SUBIR

Address A	Address B	Bytes	Bytes A→B	Bytes A←B	Packets	Packets A→B	Packets A←B
141.8.153.139	192.168.1.15	217 563 279	4 482 173	213 081 106	220 946	74 479	146 467
192.168.1.15	192.168.1.41	32 436	11 120	21 316	102	60	42
87.250.250.53	192.168.1.15	15 091	11 030	4 061	58	30	28
192.168.1.15	192.168.1.141	5 580	196	5 384	28	2	26

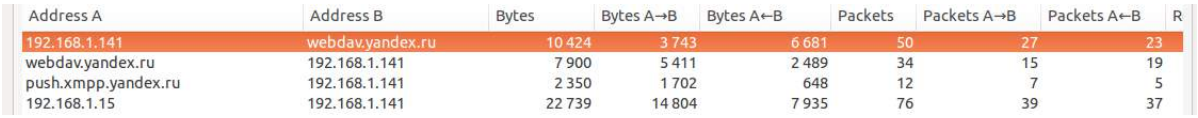
FIGURA 12 – CAPTURA *WIRESHARK* DE BYTES TRANSMITIDOS EN LA SUBIDA DEL CLIENTE DE X

[1] Los 200MB permitirán distinguir claramente los bytes correspondientes a las capturas con *Wireshark*.



Address A	Address B	Bytes	Bytes A→B	Bytes A←B	Packets	Packets A→B	Packets A←B
192.168.1.41	213.180.204.53	10 355	3 194	7 161	43	20	23
192.168.1.41	213.180.193.79	2 662	694	1 968	14	5	9
192.168.1.41	239.255.255.250	675	675	0	6	6	0

FIGURA 13 – CAPTURA *WIRESHARK* DE BYTES TRANSMITIDOS EN LA SUBIDA DEL CLIENTE DE Y



Address A	Address B	Bytes	Bytes A→B	Bytes A←B	Packets	Packets A→B	Packets A←B
192.168.1.141	webdav.yandex.ru	10 424	3 743	6 681	50	27	23
webdav.yandex.ru	192.168.1.141	7 900	5 411	2 489	34	15	19
push.xmpp.yandex.ru	192.168.1.141	2 350	1 702	648	12	7	5
192.168.1.15	192.168.1.141	22 739	14 804	7 935	76	39	37

FIGURA 14 – CAPTURA *WIRESHARK* DE BYTES TRANSMITIDOS EN LA SUBIDA DEL CLIENTE DE Z

Por tanto, puede afirmarse que el proceso de deduplicación es de tipo "***cliente – cross-user***" y sólo se realiza cuando la acción de subida de archivos se ejecuta desde sus clientes Windows y Linux nativos, en la forma indicada anteriormente, pero no así cuando se ejecuta desde la consola *web*. Este proceso, aunque es muy eficiente en cuanto al uso de ancho de banda, tiene problemas con la confidencialidad y privacidad de los datos, tal y como se detalla en [17], puesto que un atacante podría usar esta característica para:

1. Conocer qué archivos están almacenados en Yandex.Disk, observando la cantidad de bytes transmitidos al subir un archivo.
2. Obtener información de un usuario específico de Yandex.Disk. El atacante podría subir diferentes versiones de un mismo documento, presumiblemente relacionado con la víctima, y deducir, dependiendo de los bytes transmitidos, qué versión es la correcta, consiguiendo por tanto violar su privacidad.

En cuanto a la **integridad de los archivos transmitidos**, los clientes envían el *etag* y *hash* SHA-256 para cada archivo que suben a su disco en la nube. Al descargarse, el servidor envía sólo el *etag*. No ha sido posible comprobar si se usan estos valores para evaluar si los archivos han sido modificados durante la transmisión, con lo que no ha podido confirmarse si cumple o no con el requisito **R28**.

6.5.1.2.2 Almacenamiento

Según [38] hace uso del **antivirus** *Dr. Web*[2] para escanear los archivos subidos de hasta 1GB de tamaño. Para comprobar que realmente realiza un escáner en busca de *malware*, se ha creado un archivo con la cadena de pruebas EICAR [40], como la de la Figura 15, y se ha subido a la nube usando la aplicación cliente de Linux. Al acceder a la cuenta a través de la consola *web*, aparece el archivo marcado como infectado, tal y como puede verse en la Figura 15. Por tanto, puede concluirse que cumple con el requisito **R29**.

En cuanto al **cifrado de datos**, en su documentación, Yandex.Disk afirma que no cifra los datos en sus instalaciones [58] ni en sus aplicaciones cliente [38], como se comprobó en el apartado anterior. Por tanto, no cumple con el requisito **R9**, al no cifrar los datos en el cliente, ni con el **R10**, puesto que el personal interno o un atacante, que acceda a los servidores del proveedor, podría tener acceso a los datos en claro sin consentimiento del propietario.

[2] Dr. Web es un antivirus desarrollado en Rusia, siendo el más usado del país y uno de los pocos en todo el mundo que usa tecnología propia para la detección y limpieza de *malware*, cuya base de datos se actualiza en cuanto aparece una nueva identificación de virus [60].

FIGURA 15 - ARCHIVO INFECTADO CON LA CADENA EICAR, VISTO DESDE LA CONSOLA *WEB*

En lo referente a la **localización de los datos almacenados**, no se ha encontrado ninguna información al respecto en la documentación [38], con lo que no cumple con el requisito **R24**. Posiblemente estén ubicados en Rusia, donde tienen la sede, pero también podrían ubicarse en países terceros. Tampoco permite la selección de localización a sus usuarios, incumpliendo con el requisito **R25**. En la Figura 16 puede verse un conjunto de IP de Yandex.Disk localizadas todas en Rusia por http://www.ipligence.com/iplocation.

IP ADDRESS	CONTINENT	FLAG	COUNTRY	REGION	CITY
141.8.153.139	Europe		Russian Federation		Moscow
87.250.250.53	Europe		Russian Federation		Sosnovoborsk
213.180.204.53	Europe		Russian Federation		Moscow
213.180.193.79	Europe		Russian Federation		Moscow
213.180.193.1	Europe		Russian Federation		Moscow
93.158.134.1	Europe		Russian Federation		Moscow

FIGURA 16 – LOCALIZACIÓN DE ALGUNAS IP DE YANDEX.DISK

Por otro lado, Yandex.Disk indica en su documentación legal [43] que tomará "*todas las medidas razonables y llevará a cabo todas las acciones posibles para asegurar la **integridad** y **disponibilidad** de los datos de sus usuarios*", sin entrar en más detalles ni explicar que acciones y medidas son estas. Por tanto, se pone en duda el cumplimiento de los requisitos **R27** y **R30**.

6.5.1.2.3 Compartición

Según Yandex.Disk [38], los archivos y directorios pueden **compartirse de forma pública**, generando un enlace al recurso compartido con la siguiente estructura:

https://yadi.sk/d/<valor aleatorio>

Esta técnica permite a cualquiera, con acceso a un enlace válido, acceder al contenido del archivo o directorio referenciado, pero sólo en modo lectura. En la Figura 17 puede verse un ejemplo de acceso a un archivo compartido usando un enlace público.

En cuanto a la **restricción de acceso** a usuarios específicos, Yandex.Disk no permite autorizar selectivamente el acceso a archivos compartidos a ciertos usuarios. Sin embargo, sí permite hacerlo con directorios. Si un usuario quiere compartir un archivo con otros usuarios, tendrá que crear primero un directorio, copiar el archivo en dicho directorio y después asignar los permisos necesarios al directorio (*sólo lectura, acceso completo, sin permisos*), tal y como puede verse en la Figura 18. Sólo el propietario puede otorgar y denegar permisos. Esta forma de gestionar las autorizaciones de acceso, por un lado, facilita la gestión de la compartición, ya que se pueden agrupar archivos en carpetas con los mismos permisos, pero por otro le resta flexibilidad a la hora de asignar permisos a

archivos individualmente. En este caso, puede decirse que cumpliría con el requisito **R10**, si no se considera que un posible empleado malicioso de Yandex.Disk pueda acceder a la información sin permiso de su propietario, excepto si cifra aparte todos los archivos que suba.

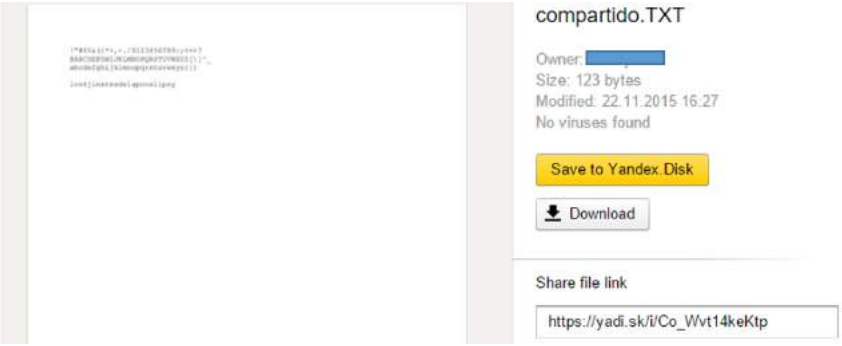


FIGURA 17 - ACCESO A UN ARCHIVO COMPARTIDO EN YANDEX.DISK

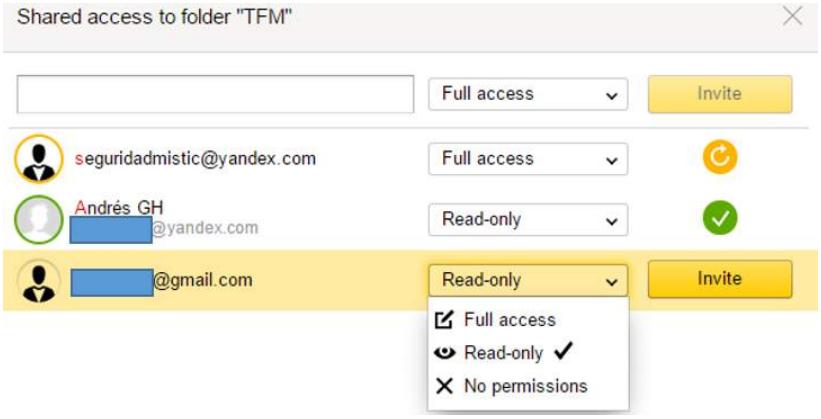


FIGURA 18 – GESTIÓN DE PERMISOS DE ACCESO A UN DIRECTORIO EN YANDEX.DISK

Desde la consola *web*, Yandex.Disk permite que un usuario pueda **ver los archivos y directorios que ha compartido**, como puede verse en la Figura 19. Por tanto, puede concluirse que cumple con el requisito R12.

FIGURA 19 - LISTA DE ARCHIVOS Y DIRECTORIOS COMPARTIDOS

En cuanto a la **indexación de los archivos por motores de búsqueda**, con las pruebas realizadas en los buscadores de Yandex, Yahoo y Google, no se ha podido encontrar ninguno de los archivos buscados, ni por su nombre ni por su identificador aleatorio, generado al compartirlo públicamente. Puede concluirse, en este caso que cumple con el requisito **R11**.

Para finalizar, señalar que Yandex.Disk, en su documentación [38], indica claramente los **métodos de compartición** que provee, con lo que cumple con el requisito **R14**.

6.5.1.2.4 Borrado

Yandex.Disk indica en su documentación [38] que cualquier elemento eliminado queda almacenado durante 30 días en la papelera de la cuenta del usuario, con el fin de poder ser restaurado en caso necesario, independientemente de si es borrado desde la consola *web* o desde una aplicación cliente. Al cabo de este tiempo, los elementos borrados se eliminan automáticamente.

Si se considera la papelera como una carpeta más del disco, entonces se podría llegar a considerar que no existe **retención de datos**. En cambio, no se indica nada, en la documentación, de lo que ocurre una vez eliminados los datos definitivamente de la papelera ni si el espacio que ocupan será sobrescrito. En caso de que un usuario dé de baja su cuenta en Yandex.Disk, la documentación [38] indica que se borrarán todos sus archivos, sin posibilidad de poder ser recuperados posteriormente, pero no se dice nada de lo que ocurre con su **espacio en disco**. Con la documentación existente no puede determinarse si se cumplen o no los requisitos **R20** y **R21**.

En cuanto a la **sincronización del borrado de archivos**, en las pruebas realizadas, se ha comprobado que cuando se borra un archivo en algún dispositivo, automáticamente se elimina del resto de dispositivos. En la Figura 20 se muestra el contenido del archivo de trazas del cliente Linux con las trazas de la sincronización del borrado entre dispositivos; en este caso se trata de la eliminación de un archivo desde la consola *web* y de su sincronización posterior en el cliente Linux. Por tanto, puede concluirse que cumple con el requisito **R19**.

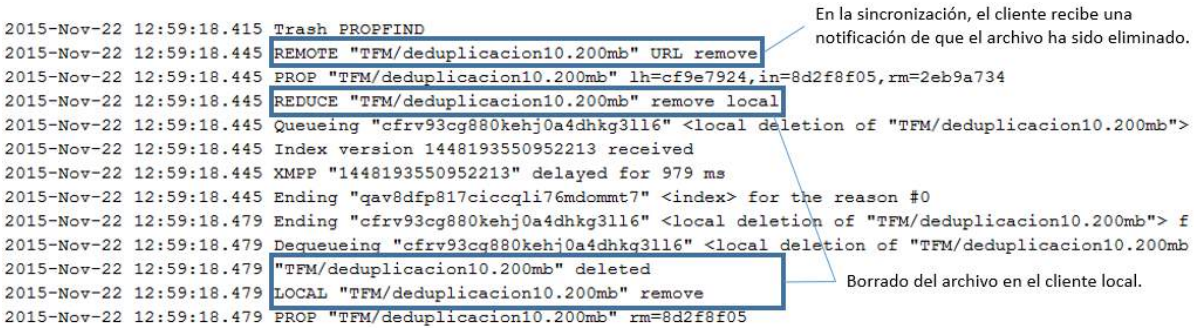


FIGURA 20 – PARTE DEL ARCHIVO DE TRAZAS CON LA SINCRONIZACIÓN DE BORRADO EN UN CLIENTE

6.5.1.2.5 Cumplimiento de la legislación

Yandex.Disk, tal y como describe en su documentación [38], está sujeta a las leyes de la Federación Rusa, que la Agencia Española de Protección de Datos (AEPD) no incluye como país con un nivel adecuado de protección [42]. Por tanto, atendiendo a lo que indica la AEPD, puede considerarse que no cumple con el requisito **R26**.

6.5.1.3 Gestión de dispositivos cliente

6.5.1.3.1 Multidispositivo

Como se dijo en la introducción, Yandex.Disk permite trabajar con diferentes dispositivos y sistemas operativos. Sin embargo, un usuario no puede ver su lista de dispositivos, activarlos ni gestionarlos desde la consola *web* del servicio. La única gestión que puede realizar un usuario es ejecutar el *logout* en remoto de todos sus dispositivos. Por tanto, puede concluirse que no cumple con los requisitos **R16**, **R17** y **R18**.

6.5.1.3.2 Actualización del software de los clientes

En cuanto a los clientes Windows y Linux, el usuario puede configurar en ambos casos la aplicación para que realice actualizaciones del software automáticamente, cumpliendo de este modo el requisito **R22**.

6.5.1.4 Conclusiones

En la Tabla 6 se resume el cumplimiento o no de los diferentes requisitos. La principal conclusión que puede obtenerse es que, en el tratamiento de la información, Yandex.Disk presenta problemas de seguridad, entre los que puede destacarse la amenaza de violación de los datos de sus usuarios, al no cifrarse la información enviada por las aplicaciones clientes hacia sus servidores, ya sea por el ataque de un empleado malicioso o a través de otro atacante que sea capaz de comprometer los servidores de Yandex.Disk. Por otro lado, la incompatibilidad de la legislación rusa con la española y la de la UE, en lo que a protección de datos personales se refiere, no permite que el producto sea adecuado para almacenar información protegida por la LOPD o la directiva 95/46/EC de 1995, entre otras; su incumplimiento puede acarrear graves sanciones económicas para el usuario del servicio de Yandex.Disk.

Procesos	Cumplimiento de los requisitos
Comunicaciones	
Conexión	• **R1**: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 con protocolo seguro TLS versión 1.2. • **R3**: Los servidores se autentican ante los clientes usando certificado digital con clave pública RSA.
Registro	• **R2**: No utiliza contraseñas robustas según definición de OWASP. • **R6**: Recolección escueta de datos. • **R7**: Solicita activación por móvil, pero sólo si el usuario lo proporciona. • **R8**: Permite enumeración de usuarios. • Los datos del registro se envían a través de TLS 1.2, pero la contraseña no se procesa con una función *hash* o similar, con lo que los servidores tienen acceso a su valor en claro.
Login	• **R4**: Autenticación básica de tipo usuario y contraseña. Creación de *token* OAuth2 para los clientes Windows y Linux. • **R5**: Soporta autenticación multifactor. • **R8**: Permite enumeración de usuarios. • Los datos del *login* se envían a través de TLS 1.2, pero la contraseña no se procesa con una función *hash* o similar, con lo que los servidores tienen acceso a su valor en claro.
Tratamiento de la información	
Transmisión de archivos	• **R9**: No cifra los archivos en el lado cliente antes de su envío a los servidores. Los servidores tienen acceso a su valor en claro. • **R15**: Uso de deduplicación de archivos *cliente – cross-user*, para los clientes Windows y Linux, que tiene problemas de confidencialidad y privacidad de datos. • **R28**: Envío de *checksum* MD5 y *hash* SHA-256 para los archivos enviados al servidor. Los clientes reciben sólo el *checksum* MD5 al descargar un archivo.
Almacenamiento	• **R9**: No cifra los archivos en el lado cliente. • **R10**: Al no cifrar los datos en el lado cliente, permite a los servidores tener acceso en claro de los archivos almacenados. • **R24**: No proporciona información sobre la localización de los datos en las instalaciones del proveedor. • **R25**: Los usuarios no pueden seleccionar la localización de sus datos. • **R27**: En la documentación no habla explícitamente de la realización de ningún tipo de *backup* de los datos almacenados de sus usuarios.

Procesos	Cumplimiento de los requisitos
	• **R29**: Uso del antivirus *Dr. Web* para escanear los archivos almacenados de hasta 1GB. • **R30**: El proveedor indica que tomará "*todas las medidas razonables y llevará a cabo todas las acciones posibles para asegurar la **integridad** y **disponibilidad** de los datos de sus usuarios*".
Compartición	• **R10**: La compartición de archivos y carpetas se realiza a través de enlaces. Sólo permite restringir el acceso y otorgar permisos a usuarios específicos sobre carpetas. • **R11**: No permite la indexación de los archivos por motores de búsqueda. • **R12**: Los usuarios tienen acceso a un listado de recursos compartidos. • **R14**: El proveedor indica claramente los métodos de compartición.
Borrado	• **R19**: Sincronización de la eliminación de archivos entre todos los dispositivos conectados a la cuenta. • **R20**: No ha podido determinarse si se sobrescribe el espacio que ocupaban los datos borrados, al ser eliminados definitivamente. • **R21**: Los archivos eliminados se guardan en la papelera de la cuenta del usuario hasta que el usuario los elimine definitivamente o pasen 30 días. No se indica si existe algún periodo de retención posteriormente.
Cumplimiento de la Legislación	• **R26**: La AEPD no considera que Rusia, sede del proveedor, sea un país con un nivel adecuado de protección.
Gestión de dispositivos	
Gestión multidispositivo	• **R16**: No existe listado de dispositivos registrados con una cuenta de usuario. • **R17**: El usuario no puede activar ni desactivar ninguno de sus dispositivos manualmente. • **R18**: El usuario no puede seleccionar el nombre de sus dispositivos asociados con su cuenta.
Actualización del software cliente	• **R22**: El software de los clientes puede actualizarse de forma automática o a instancias del usuario. • **R23**: No se han encontrados registros de actualizaciones.

TABLA 6 –CUMPLIMIENTO DE LOS REQUISITOS POR PARTE DE YANDEX.DISK

6.5.2 CloudMe

CloudMe (https://www.cloudme.com/) es un producto de almacenamiento en la nube perteneciente y operado por la compañía CloudMe AB ubicada en Suecia. Se vende como un producto europeo que cumple con la legislación de la Unión Europea en materia de seguridad y privacidad de datos [46], con el fin de hacerlo atractivo para los consumidores de la propia UE y de otros países con legislaciones menos restrictivas. En el 2014 fue reconocida entre las 30 primeras compañías tecnológicas emergentes de Europa, según su propia *web*.

CloudMe ofrece almacenamiento gratuito en la nube con capacidad de 3GB por cuenta, aunque puede ampliarse gratuitamente hasta 16GB mediante invitaciones a amigos. Existe la posibilidad de comprar almacenamiento extra, para los consumidores privados, de 10GB a 10€ anuales, 25GB a 40€, 100GB a 80€, 200GB a 140€ y 500GB a 300€ anuales [46]. Para las empresas, tienen tres ofertas: 1TB y 5 usuarios a 1.490€, 2TB y 15 usuarios a 2.790€ y 5TB y 50 usuarios a 7.590€ anuales.

Según su documentación, permite gestionar los archivos de sus usuarios desde aplicaciones clientes instaladas en diferentes dispositivos conectados a Internet:

- Ordenadores personales con Microsoft Windows, Linux o Mac OS X.
- Dispositivos móviles con Android o iOS.
- Televisiones inteligentes con servicios de Samsung Smart TV, WD TV o Google TV.

CloudMe soporta los protocolos WebDAV, SOAP y RESTful, proporcionando las API para poder implementar aplicaciones clientes que interactúen con el servicio de almacenamiento en la nube. Puesto que soporta el protocolo WebDAV, hace posible que un usuario pueda conectarse desde su sistema operativo a su almacenamiento en la nube como si fuera una unidad de red más, sin la necesidad de instalar ningún tipo de cliente [46].

En cuanto a la documentación ofrecida, ésta es muy escasa y remiten principalmente a un foro [47] en el que se intenta dar respuesta a las preguntas lanzadas por sus usuarios. Además, la búsqueda de información en motores de búsqueda como Google o Bing devuelve muy pocos resultados en comparación con otros productos de almacenamiento en la nube. Esta desventaja puede hacer dudar a cualquier usuario, a la hora de escogerlo como almacenamiento para su información.

6.5.2.1 Comunicaciones

6.5.2.1.1 Conexión

En las pruebas realizadas, para **asegurar** las **comunicaciones** entre los clientes y sus servidores, CloudMe usa el protocolo seguro TLS, versión 1.2. En todas las comunicaciones, sus servidores han escogido la **suite de cifrado** TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, durante el proceso de negociación de claves (ver captura en la Figura 21 y sus características en el Anexo A), aunque sus clientes siempre han presentado las que se muestran en la captura de la Figura 22. Por tanto, cumple con el requisito **R1**, al proporcionar **confidencialidad** e **integridad en las comunicaciones**.

Los **servidores** utilizan para **autenticarse** ante los clientes un certificado digital con clave pública RSA y firmado por una autoridad de certificación reconocida, como el de la Figura 23. Por tanto, puede deducirse que cumple con el requisito **R3**.

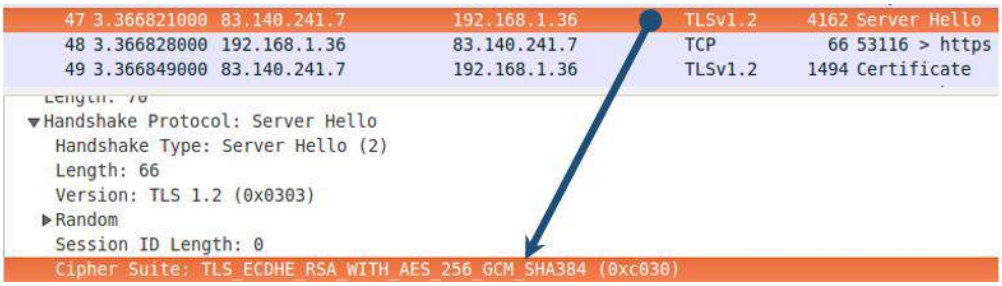


FIGURA 21 – SUITE DE CIFRADO ESTABLECIDA EN LA CONEXIÓN TLS DEL CLIENTE UBUNTU

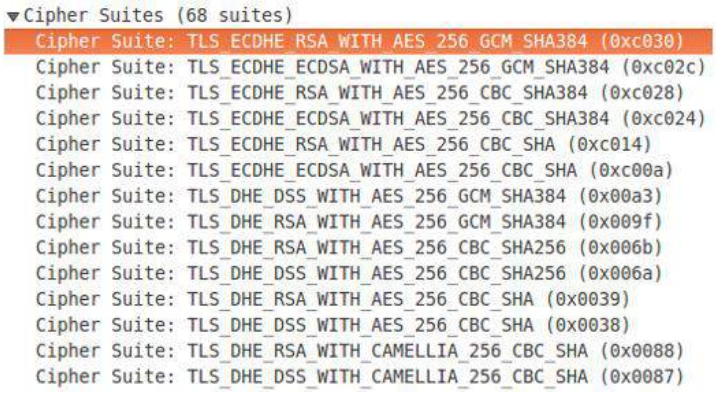


FIGURA 22 - ALGUNAS SUITES DE CIFRADO OFRECIDAS POR EL CLIENTE LINUX EN LA CONEXIÓN TLS

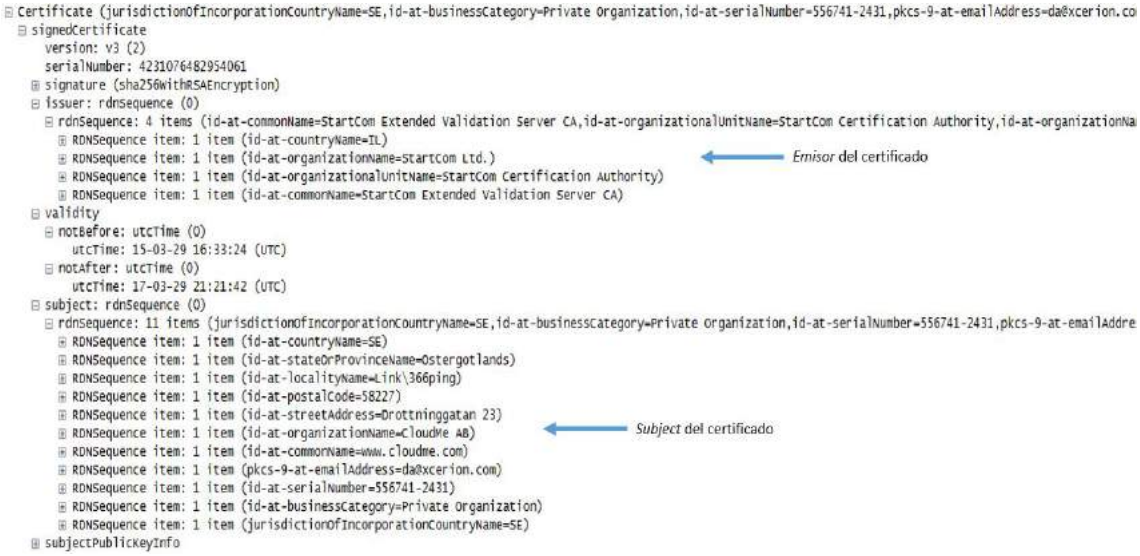


FIGURA 23 - CAPTURA DEL CERTIFICADO DURANTE UNA CONEXIÓN DEL CLIENTE WINDOWS

6.5.2.1.2 Registro

La **creación de una cuenta** en CloudMe debe realizarse desde su página *web*. El formulario de registro requiere la siguiente información: nombre y apellido, nombre de usuario, contraseña, repetición de contraseña, cuenta de correo electrónico de contacto, país y la aceptación de las condiciones de uso. Puede decirse que la **recolección de información** es muy escueta, con lo que se concluye que cumple con el requisito **R6**. Sin embargo, no solicita ningún número de teléfono móvil al que enviar un código de validación ni la introducción de ningún *captcha* ni de cualquier otra medida extra de seguridad, lo que puede ser aprovechado por un atacante para crear nuevos usuarios de forma indiscriminada, tal y como se verá más adelante.

La **contraseña**, a pesar de enviarse a través de una conexión segura TLS, es recibida por los servidores de CloudMe sin procesar por una función *hash* o similar, con lo que tendrán acceso a la contraseña en claro [18], como puede verse en la captura de una petición de registro de la Figura 24. Es decir, tanto el personal interno del proveedor como un atacante podrían tener **acceso a las contraseñas** de las cuentas de usuarios nuevos y así a su contenido. A pesar de esto, según lo descrito en el foro de CloudMe [47], en el servidor se almacena el *hash* MD5 de la contraseña.

FIGURA 24 – CAPTURA DE UNA PETICIÓN DE REGISTRO EN CLOUDME CON ZAP

CloudMe no está protegido contra la **enumeración** de usuarios existentes, es decir, no cumple con el requisito **R8**, como se demuestra a continuación. Durante la etapa de registro, el formulario da pistas de los nombres de usuario disponibles y cuáles se encuentran dados de alta, como en el ejemplo de la Figura 25. El formulario de registro, para averiguar si un nombre de usuario ya existe o está disponible, lanza una petición Ajax al servidor, por cada letra que se escribe en el campo del nombre de usuario. El servidor responde a la petición indicando si el nombre está "ocupado" o "disponible". La URL utilizada en la petición tiene el siguiente formato:

```
https://www.cloudme.com/ajax/username_check.php?username=<nombre usuario>
```

Con esta información, un atacante podría crear un programa sencillo que lanzara peticiones al servidor para averiguar si una serie de usuarios ya existen en el servicio o bien se encuentran disponibles, sacados por ejemplo de un diccionario de nombres, es decir los **enumera**. En la Figura 26 se muestra parte de la salida de un programa de este estilo, implementado para el análisis, con el que se ha podido obtener una lista de usuarios que ya tienen cuenta en CloudMe y otra lista de nombres disponibles, usando como diccionario un listado de nombres propios obtenido de Internet.

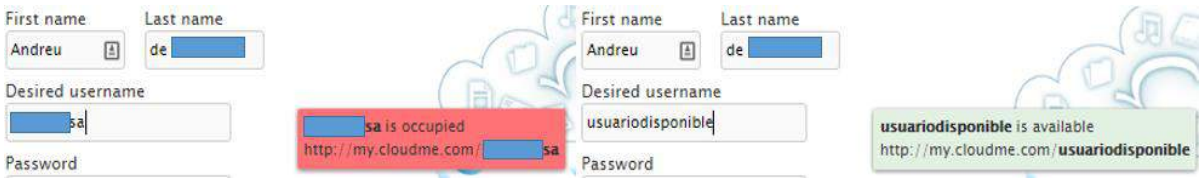


FIGURA 25 – ENUMERACIÓN EN EL REGISTRO DE USUARIOS NUEVOS EN CLOUDME

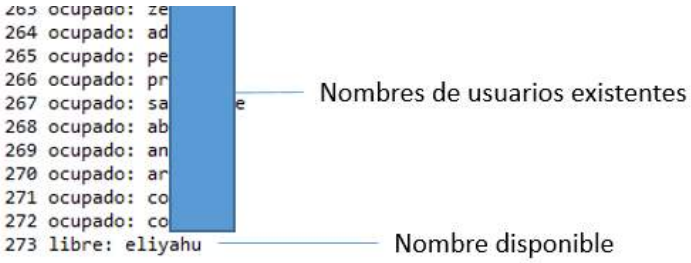


FIGURA 26 – SUBCONJUNTO DE NOMBRES DE USUARIOS OCUPADOS Y DISPONIBLES EN CLOUDME

En cuanto a la **selección de la contraseña**, ésta debe tener una longitud mínima de cinco caracteres, pero no indica cuál debe ser la máxima; durante el análisis se ha creado un usuario con una contraseña de mil caracteres, con la que posteriormente ha sido posible autenticarse. Se permite la creación de contraseñas con repeticiones de caracteres (como la 111111111), iguales al nombre del

usuario o simplemente la palabra *password*. Es decir, no cumple con la mayoría de las características sugeridas por OWASP en [48], ni por tanto con el requisito **R2**.

Una vez finalizado el proceso de registro, el proveedor envía un correo electrónico confirmando su creación, pero en ningún caso solicita al usuario su **confirmación**, incumpliendo por tanto con los requisitos **R7**. El proveedor tampoco confirma la existencia de la cuenta de correo electrónico suministrada por el usuario, con lo que es posible proporcionar direcciones de correo falsas.

Para finalizar, tal y como se ha comentado al principio, **un atacante puede crear nuevos usuarios de forma indiscriminada en el proveedor**. Éste se aprovechará de las debilidades que se han estudiado (enumeración, no existencia de *captcha* ni móvil de validación durante el registro, falta de envío de correo de activación de cuenta), que permiten lanzar peticiones HTTP de registro de nuevos usuarios al servidor, quien las acepta y procesa. El atacante podría usar estas cuentas para almacenar, por ejemplo, información ilícita, lanzar ataques a otras personas o simplemente crear miles de cuentas sin uso, que pueden suponer un problema de gestión para el proveedor de CloudMe e incluso una denegación de servicio. En la Figura 27 se muestra un ejemplo de la salida del programa anterior, en la que puede verse la petición de registro de nuevo usuario para uno de los nombres disponibles, en este caso "*eitan*". En la Figura 28 puede verse su disco desde la consola *web*.

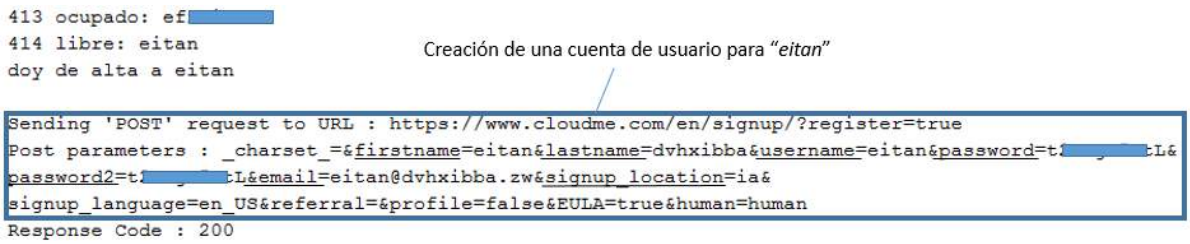


FIGURA 27 – CREACIÓN DE NUEVA CUENTA MEDIANTE EL LANZAMIENTO DE UNA PETICIÓN HTTP

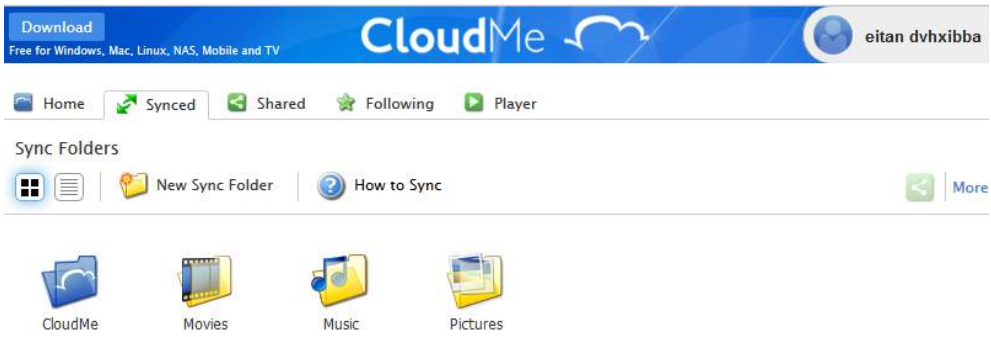


FIGURA 28 – DISCO DE CLOUDME DEL USUARIO *EITAN* CREADO AUTOMÁTICAMENTE

6.5.2.1.3 Login

La **autenticación** en CloudMe es de tipo usuario y contraseña, tanto para la consola *web* como en los clientes Windows y Linux. Puede concluirse, por tanto, que cumple con el requisito **R4**, ya que existe autenticación por parte del usuario en todos los casos. Sin embargo, no soporta la **autenticación multifactor** [47], con lo que no se cumple el requisito **R5**.

Durante la fase de ***login***, el nombre de usuario y la contraseña se envían al proveedor a través de la conexión segura, además de calcular el *hash* MD5 de la contraseña en el cliente antes de mandarla al servidor. Para el cálculo del valor del *hash* se realiza la siguiente operación, tal y como puede verse en el código JavaScript de la Figura 29:

```
md5(concatenar (<nombre de usuario>, ":os@xcerion.com:", <contraseña>))
```

En la Figura 30 puede verse una traza de Firefox con la petición de *login* de un usuario, donde la contraseña aparece resumida después de aplicarle la función *hash* MD5.

FIGURA 29 - CÓDIGO JAVASCRIPT UTILS.MD5 QUE RESUME LA CONTRASEÑA ANTES DE ENVIARLA

FIGURA 30 – TRAZA DE FIREFOX CON EL *HASH* MD5 DE UNA CONTRASEÑA

A diferencia del formulario de registro, el de *login* en la consola *web* no permite la **enumeración** de usuarios. Si se introduce un usuario o contraseña erróneos, siempre regresa el mismo mensaje de error. En conclusión, el formulario de *login* en la consola *web* cumple con el requisito **R8**.

6.5.2.2 Tratamiento de la información

6.5.2.2.1 Transmisión de archivos

Toda la transmisión de archivos entre los servidores de CloudMe y sus clientes se realiza a través de una conexión segura TLS, con lo que la transmisión queda asegurada. CloudMe indica que **no cifra de forma nativa los archivos** en el lado cliente antes de enviarlos a sus servidores. Si un usuario quiere que sus archivos se cifren, CloudMe recomienda el uso de aplicaciones de terceros, para realizar el proceso de cifrado en el lado cliente [47].

Se han realizado un conjunto de pruebas para confirmar este extremo en los clientes *web*, Linux y Windows, que concluyen que no cumple con el requisito **R9**, ya que **no cifra los datos en sus clientes** antes de transmitirlos. En la Figura 31, se muestra la captura del contenido de un archivo de texto plano subido a CloudMe desde su consola *web* y, en la Figura 32, la captura de un archivo subido por un cliente Windows y descargado desde la *web*. Es decir, el personal interno o un atacante podrían tener acceso a la información que llega a CloudMe [18]. Con esto, también peligra el cumplimiento del requisito **R10**, puesto que se podría tener **acceso al contenido** de los archivos **sin autorización** para ello.

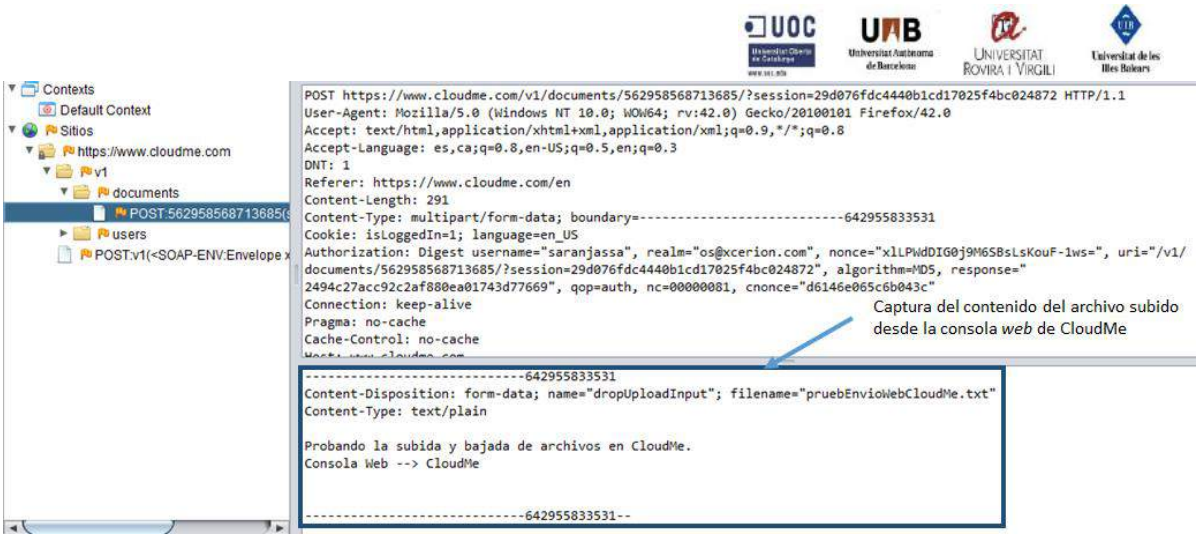


FIGURA 31 – CAPTURA CON ZAP DE LA SUBIDA DE UN ARCHIVO DE TEXTO DESDE LA CONSOLA *WEB*

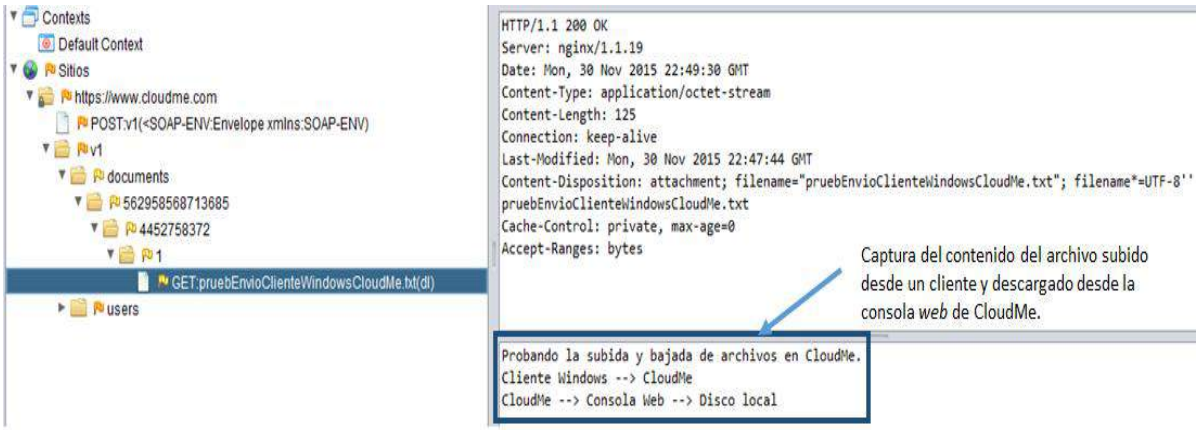


FIGURA 32 - CAPTURA DE DESCARGA DESDE LA *WEB* DE UN ARCHIVO SUBIDO CON UN CLIENTE

En la documentación de CloudMe no se menciona en ningún momento el uso del **proceso de deduplicación** en su servicio. En el estudio de 2012 llevado a cabo en [17] se menciona que CloudMe no deduplica. Para confirmar que sigue siendo así, se han realizado pruebas en las que se ha comprobado que no realiza la deduplicación en cliente; siempre sube los archivos completos, aunque su contenido sea exactamente el mismo a uno ya existente, bien en la misma cuenta de usuario o en la de otro.

En las pruebas de **deduplicación** realizadas, se ha subido el mismo archivo de 200MB[3] dos veces (con nombres diferentes) a la misma cuenta X de CloudMe por un lado y después a otra cuenta diferente Y. En todos los casos, como puede verse en los bytes transmitidos de la Figura 33, Figura 34 y Figura 35, el archivo se sube completo al servidor, con lo que queda descartada la deduplicación en el lado cliente. Sin embargo, no se ha podido averiguar si realiza deduplicación en el servidor, con lo que a tenor de la ausencia total de documentación al respecto por parte de CloudMe y a lo indicado en [17], puede descartarse el uso de deduplicación para almacenar la información en sus servidores. Por tanto, cumple con el requisito **R15**.

[3] Los 200MB permitirán distinguir claramente los bytes correspondientes a las capturas con *Wireshark*.

Address A	Address B	Bytes	Bytes A→B	Bytes A←B	Packets	Packets A→B	Packets A←B
83.140.241.10	192.168.1.143	136 887 217	3 365 804	133 521 413	91 456	49 981	41 475
83.140.241.9	192.168.1.143	77 832 826	2 087 521	75 745 305	47 258	31 159	16 099
83.140.241.8	192.168.1.143	13 236	5 670	7 566	80	28	52
192.168.1.1	192.168.1.143	10 030	10 030	0	17	17	0
83.140.241.14	192.168.1.143	5 020	3 943	1 077	9	6	3

FIGURA 33 – CAPTURA *WIRESHARK* DE SUBIDA DEL PRIMER ARCHIVO DE X CON CLIENTE LINUX

Address A	Address B	Bytes	Bytes A→B	Bytes A←B	Packets	Packets A→B	Packets A←B	Rel Start	Duration	bp
83.140.241.10	192.168.1.15	219 857 904	6 567 562	213 290 342	235 147	89 632	145 515	4.962806000	233.4999	
83.140.241.7	192.168.1.15	160 253	122 988	37 265	419	221	198	82.931125000	214.3836	
83.140.241.8	192.168.1.15	37 744	27 933	9 811	135	64	71	2.283301000	174.6552	
192.168.1.1	192.168.1.15	2 360	2 360	0	4	4	0	5.454060000	0.0000	18

FIGURA 34 – CAPTURA *WIRESHARK* DE SUBIDA DEL SEGUNDO ARCHIVO DE X CON CLIENTE WINDOWS

Address A	Address B	Bytes	Bytes A→B	Bytes A←B	Packets	Packets A→B	Packets A←B	Rel Start
83.140.241.8	192.168.1.143	82 545 948	2 034 808	80 511 140	55 007	30 333	24 674	4,2481450
83.140.241.9	192.168.1.143	70 620 047	1 843 268	68 776 779	44 315	27 362	16 953	145,455373(
83.140.241.10	192.168.1.143	61 813 583	1 491 776	60 321 807	43 760	22 145	21 615	7,8549570
192.168.1.1	192.168.1.143	7 080	7 080	0	12	12	0	4,6800160

FIGURA 35 – CAPTURA *WIRESHARK* DE LA SUBIDA DEL ARCHIVO DE Y DESDE EL CLIENTE LINUX

En cuanto a la **integridad de los archivos transmitidos**, el cliente almacena en una BDD SQLite (llamada *cache.db*) el *checksum* MD5 de todos los archivos que sincroniza. En el **proceso de subida** de un archivo, los clientes reciben su *checksum* MD5 como parte de la respuesta del servidor, tal y como puede verse en las trazas del cliente Linux de la Figura 36. Aunque no es concluyente, podría decirse que el cliente estaría comparando la respuesta del servidor con el valor del *checksum*, calculado antes de iniciar el proceso de subida, para verificar su integridad. En el **proceso de descarga**, el cliente envía al servidor un mensaje de éxito, al finalizar la descarga, con el nombre del archivo y el *checksum* MD5 de su contenido (excepto cuando la descarga se realiza desde la consola *web*), como en la Figura 37, con lo que podría suponerse, ya que no se ha encontrado documentación, que el servidor realiza una verificación de la integridad parecida a la del lado cliente durante la subida.

En conclusión, parece que se verifica la integridad durante la transmisión de archivos, aunque, al no ser posible probarlo con precisión, puesto que no se tiene acceso al código fuente ni se ha encontrado documentación que lo explique, no puede confirmarse el cumplimiento del requisito **R28**.

```
<atom:entry xmlns:os="http://a9.com/-/spec/opensearch/1.1/" xmlns:dc="http:/
"http://www.w3.org/2005/Atom">
    <atom:title>2015-11-30.txt</atom:title>
    <atom:published>2015-12-13T08:05:57Z</atom:published>
    <atom:updated>2015-12-13T08:05:57Z</atom:updated>
    <atom:link length="3605" type="text/plain" href="https://os.cloudme.com/
    <atom:id>mid:10970e9c2@xios.xcerion.com</atom:id>
    <dc:folder>562958568846365</dc:folder>
    <dc:document>4453362114</dc:document>
    <dc:md5>27c0800916152b2965198276eb2ab2be</dc:md5>
</atom:entry>
```

FIGURA 36 – RESULTADO DEVUELTO POR EL SERVIDOR AL SUBIR UN ARCHIVO DESDE UN CLIENTE

```
onDownloadSuccess:  "PruebEnvioWebBajadaClienteWindows.txt"  |  "1384824e5384de317395fb19dfd642e5"
```

FIGURA 37 – *HASH* MD5 CALCULADO EN LA BAJADA DE UN ARCHIVO DESDE UN CLIENTE

6.5.2.2.2 Almacenamiento

CloudMe permite almacenar archivos infectados con ***malware*** [47]. Pasa la responsabilidad al programa **antivirus** que tengan instalados sus usuarios. Para probarlo, se ha subido el archivo con la cadena EICAR [40] desde la aplicación cliente de Linux. Al acceder desde la consola *web*, el archivo no está marcado como infectado ni se advierte de su contenido cuando se descarga. Por tanto, se concluye que no cumple con el requisito **R29**.

En cuanto al **cifrado de datos**, CloudMe indica que no cifra los archivos de sus usuarios en sus instalaciones ni en sus aplicaciones cliente [47], como se comprobó en el apartado anterior. Por tanto, no cumple con el requisito **R9**, al no cifrar los datos en el cliente, ni con el **R10**, puesto que el personal interno o un atacante podrían acceder a los datos en claro en el servidor sin consentimiento de su propietario.

Con respecto a la **localización de sus servidores**, CloudMe indica en su documentación que todos sus sistemas de almacenamiento se encuentran situados en el sur de Suecia [46] [47]. Durante las pruebas, se ha podido verificar que las direcciones IP, con las que se conectan los clientes, pertenecen a Suecia (ver salida *whois* de la Figura 38). Por tanto, si se considera que es cierto lo que se indica en la documentación, cumple con el requisito **R24**. Sin embargo, el usuario **no puede escoger la localización** en la que se almacenarán sus archivos, incumpliendo el requisito **R25**.

```
inetnum:        83.140.241.0 - 83.140.241.255
netname:        XCERION-NET
descr:          Xcerion AB

country:        SE
admin-c:        PORT80-RIPE
```

FIGURA 38 – PARTE DE LA SALIDA DE WHOIS PARA LAS IP DE CLOUDME

Para finalizar, CloudMe indica en su política de privacidad, en el apartado de **seguridad de datos e integridad**, que utiliza dispositivos de seguridad y tecnología que cumplen en todo momento con las leyes que son aplicables y con los estándares de la industria para proteger la información de pérdidas, destrucción, abusos, divulgación no permitida y acceso o modificación no autorizados. Sin embargo, no explica en ningún caso cómo lleva a cabo lo que afirma, poniendo en duda el cumplimiento de los requisitos **R27** y **R30**.

6.5.2.2.3 Compartición

Toda la **compartición de recursos** (archivos y carpetas) se realiza con el método *WebShares* [46]. Cuando un usuario quiere compartir un recurso, se crea un *WebShare*, al que se accede mediante un enlace desde cualquier navegador *web*, sin ser necesario tener cuenta en CloudMe y cuya estructura es una de las siguientes:

https://my.cloudme.com/#nombreUsuarioPropietario/nombreRecursoCompartido
https://my.cloudme.com/nombreUsuarioPropietario/nombreRecursoCompartido

Esta forma de compartir recursos conlleva **problemas para la confidencialidad y privacidad** de los datos de sus usuarios. Un atacante podría lanzar un ataque para averiguar qué recursos comparte un usuario determinado del servicio, invocando repetidamente a la misma URL con nombres de recursos diferentes. Si encuentra recursos compartidos sin ninguna contraseña (ver como se protegen los recursos compartidos más adelante), será fácil acceder a la información, en caso contrario, será suficiente con hacerse con la contraseña para revelar su contenido.

Cuando se quiere **compartir un recurso**, el usuario puede seleccionar con quién lo comparte: otros usuarios de CloudMe o cuentas de correo electrónico, *Facebook* o *Twitter*, como se ve en la Figura 39. Inicialmente, cualquier recurso compartido podrá ser **seguido** por cualquier usuario de CloudMe, permitiendo ver siempre la última versión subida por su propietario.

Para **compartir una carpeta**, el usuario podrá decidir cómo quiere compartirla, tal y como puede verse en la Figura 40. A continuación, se resumen las diferentes opciones de compartición:

- *WebShare*. Permite ver su contenido a cualquiera que acceda a su enlace. Sólo el propietario puede modificar lo que contiene. Si el propietario marca que se comparte la carpeta de forma privada y se le asigna una contraseña, quien quiera acceder a su contenido tendrá que recibir la invitación como usuario CloudMe o acceder a la carpeta a través del enlace del *WebShare* e introducir la contraseña asignada, como en la Figura 41, la cual se cifra antes de ser enviada. Sin embargo, si el propietario de una carpeta privada comparte uno de sus archivos, éste podrá verse públicamente sin necesidad de contraseña.
- *WebShare+*. Tiene la misma funcionalidad que *WebShare*, pero sólo puede compartirse de forma privada y añade la posibilidad de que los usuarios puedan subir archivos a la carpeta, pero sin modificar ni eliminar los existentes, tarea que sólo puede realizar el propietario.
- *Collaboration*. Pensada para el trabajo colaborativo entre diferentes usuarios. Tiene la misma funcionalidad de *WebShare+*, pero permite modificar los archivos existentes, aunque sólo el propietario puede eliminarlos.

FIGURA 39 - COMPARTIR UN RECURSO CON OTROS USUARIOS

En ninguno de los métodos anteriores se **autoriza el acceso** a una carpeta a usuarios específicos. Por tanto, si quiere autorizarse el acceso a un conjunto de usuarios restringidos, debe compartirse la carpeta de forma privada y protegerla con una contraseña; quien la posea estará autorizado a abrirla, independientemente de que tenga cuenta CloudMe o no. Esta gestión de las autorizaciones tiene una serie de debilidades, entre las que pueden destacarse:

- Las **contraseñas deben difundirse a los usuarios autorizados**, por lo que un atacante podría robarla si no se hace de forma segura.
- Cada vez que se quiere **denegar el acceso** a un usuario, el propietario debe cambiar la contraseña y reenviarla al resto de usuarios que comparten el recurso.
- Nadie puede asegurar que un usuario autorizado no difunda la contraseña anónimamente a terceros, **permitiendo a cualquiera acceder al contenido e incluso cambiarlo**.

Con todo esto, puede concluirse que la compartición no cumple con el requisito **R10**, ya que, si bien el propietario es el único que puede asignar y cambiar las contraseñas de acceso a los recursos

compartidos, una vez asignadas, pierde el poder de decidir quién tiene acceso, al menos hasta que vuelva a cambiarlas.

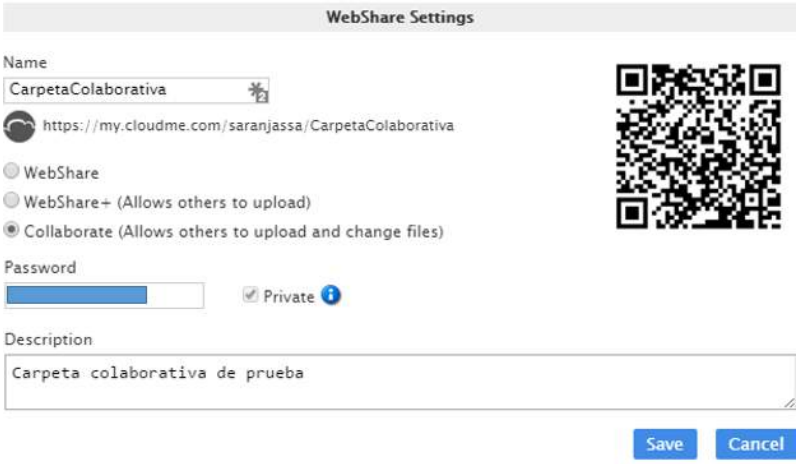


FIGURA 40 – CONFIGURACIÓN DE CARPETA COMPARTIDA DESDE LA CONSOLA *WEB* DEL PROPIETARIO

FIGURA 41 – PASSWORD DE ACCESO A UNA CARPETA PRIVADA DESDE EL ENLACE DEL *WEBSHARE*

Desde la consola *web*, CloudMe permite que un usuario pueda **ver los archivos y carpetas** que ha **compartido**, como en el ejemplo de la Figura 42. Por tanto, puede concluirse que cumple con el requisito **R12**.

En cuanto a la **indexación de archivos** por algún motor de búsqueda, con las pruebas realizadas en los buscadores de Google, Yahoo, Bing y Yandex no ha sido posible encontrar ninguno de los archivos buscados ni sus enlaces, cumpliendo con el requisito **R11**.

Para finalizar, cabe señalar que CloudMe **indica los métodos de compartición** que provee [46] [47], cumpliendo por tanto con el requisito **R14**.

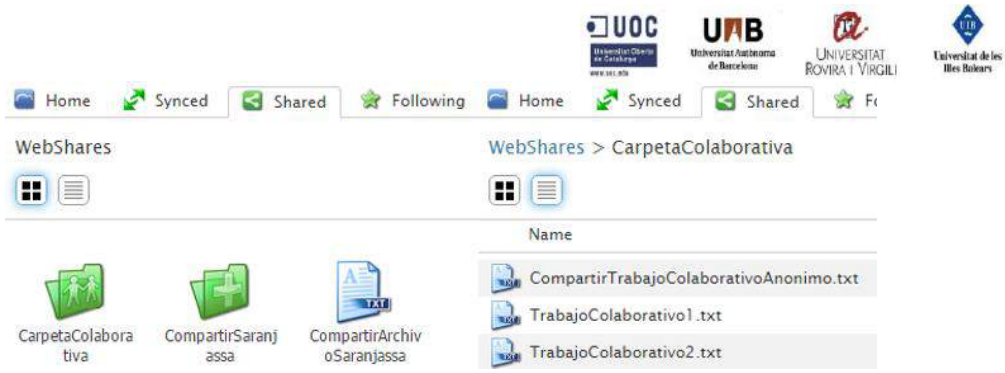


FIGURA 42 - ARCHIVOS Y CARPETAS COMPARTIDOS POR UN USUARIO

6.5.2.2.4 Borrado

CloudMe indica en [47] que cualquier elemento **eliminado** queda almacenado en la papelera de la cuenta de usuario durante 60 días, con el fin de poder ser restaurado en caso de borrado accidental, independientemente de si es borrado desde la consola *web* o un cliente. Al cabo de ese tiempo, los elementos se eliminan automáticamente de la papelera. Los usuarios no pueden vaciar la papelera cuando desean y la única operación que se permite es la restauración de elementos eliminados. Si se considera el hecho de que el usuario no puede decidir cuándo limpiar la papelera, teniendo que esperar 60 días a que esto suceda por cada elemento, puede concluirse que existe un **periodo de retención** por ese tiempo. Por tanto, se considera entonces que no cumple con el requisito **R21**.

Por otro lado, CloudMe indica en su documentación que una vez **se eliminan definitivamente** los datos de la papelera, estos se borran de todos sus sistemas, pero no menciona si el espacio que ocupaban será sobrescrito. Si un **usuario se da de baja** de CloudMe, dejará de tener acceso a todos sus datos y su cuenta no podrá ser reutilizada, pero en la documentación no se menciona lo que ocurre con sus archivos ni con su espacio de disco. Por tanto, con la información existente no puede determinarse si se cumple o no con el requisito **R20**.

En cuanto a la **sincronización del borrado de archivos**, en las pruebas realizadas, se ha comprobado que cuando se borra un archivo o carpeta, automáticamente se elimina del resto de dispositivos. En la Figura 43 pueden verse las trazas generadas por el cliente Linux durante una sincronización de borrado; en este caso se ha eliminado un archivo en la consola *web* del usuario y se ha sincronizado con el cliente Linux. Puede concluirse que cumple con el requisito **R19**.

FIGURA 43 – TRAZAS DEL CLIENTE LINUX EN LA SINCRONIZACIÓN DEL BORRADO DE UN ARCHIVO

6.5.2.2.5 Normativa

CloudMe, tal y como describe en su documentación [46], está sujeto a la **jurisdicción** de Suecia y la **Unión Europea**, en lo que a protección de datos se refiere. Puesto que la norma europea rige tanto en España como en Suecia [49], se concluye que cumple con el requisito **R26**.

6.5.2.3 Gestión de dispositivos cliente

6.5.2.3.1 Multidispositivo

Como se mencionó en la introducción, CloudMe permite trabajar con diferentes dispositivos y sistemas operativos. Sin embargo, un usuario no puede ver su listado de **dispositivos**, activarlos ni gestionarlos desde la consola *web* del servicio. Por tanto, puede concluirse que no cumple con los requisitos **R16**, **R17** y **R18**.

6.5.2.3.2 Actualización del software de los clientes

En los clientes Windows y Linux, el usuario puede configurar la aplicación para que realice **actualizaciones automáticas** del software de las aplicaciones o bien que se le notifique, para poder decidir cuándo ejecutar la actualización, cumpliendo de este modo con el requisito **R22**.

En cuanto al **registro de cambios**, no ha sido posible encontrar en la documentación de CloudMe nada que indique que se lleva un control de cambios del software cliente. Tampoco ha sido posible realizar pruebas en este sentido, puesto que no se ha liberado ninguna versión nueva de los clientes durante el análisis. Con esto, no puede determinarse si se cumple con el requisito **R23**.

6.5.2.4 Conclusiones

En la Tabla 7 se resume el cumplimiento o no de los diferentes requisitos. La principal conclusión que puede obtenerse es que CloudMe puede presentar problemas de seguridad en el tratamiento de la información y creación de nuevas cuentas. Aunque presenta algunos puntos fuertes, como es el hecho de cumplir con la legislación de la Unión Europea, la cual rige también en España. Entre los problemas mencionados, puede destacarse:

- El proceso de registro permite **enumerar** fácil y automáticamente a conjuntos importantes de sus usuarios.
- El mismo proceso de registro posibilita la creación masiva de nuevas cuentas de usuarios con un sencillo programa y sin ningún tipo de control por parte del proveedor. Esto permitiría lanzar un ataque de **denegación de servicio**, en el que comprometería la provisión de almacenamiento para usuarios lícitos.
- La **amenaza de violación de los datos** de sus usuarios, al no cifrarse la información enviada por las aplicaciones clientes hacia sus servidores, ya sea por el ataque de un empleado malicioso o a través de otro atacante que sea capaz de comprometer los servidores de CloudMe. Tampoco cifra los datos en sus instalaciones, aunque no se presentaba como un requisito a cumplir.

Procesos	Cumplimiento de los requisitos
Comunicaciones	
Conexión	• **R1**: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 con protocolo seguro TLS versión 1.2. • **R3**: Los servidores se autentican ante los clientes usando certificado digital con clave pública RSA.
Registro	• **R2**: No utiliza contraseñas robustas según definición de OWASP. • **R6**: Recolección escueta de datos. • **R7**: No solicita activación de la cuenta de usuario. • **R8**: Permite enumeración de usuarios. • Los datos del registro se envían a través de TLS 1.2, pero la contraseña no se procesa con una función *hash* o similar, con lo que los servidores tienen acceso a su valor en claro.

Procesos	Cumplimiento de los requisitos
Login	• **R4**: Autenticación básica de tipo usuario y contraseña. La contraseña es procesada con una función *hash* MD5 antes de ser enviada a los servidores. • **R5**: No soporta autenticación multifactor. • **R8**: No permite enumeración de usuarios.
Tratamiento de la información	
Transmisión de archivos	• **R9**: No cifra los archivos en el lado cliente antes de su envío a los servidores. Los servidores tienen acceso a su valor en claro. • **R15**: No usa deduplicación para almacenar los archivos. • **R28**: Intercambio del *checksum* MD5 de los archivos durante su transmisión.
Almacenamiento	• **R9**: No cifra los archivos en el lado cliente. • **R10**: Al no cifrar los datos en el lado cliente, permite a los servidores tener acceso en claro de los archivos almacenados. • **R24**: Según su documentación, los datos de sus usuarios se guardan en sus instalaciones situadas en el sur de Suecia. • **R25**: Los usuarios no pueden seleccionar la localización de sus datos. • **R27**: En la documentación no habla explícitamente de la realización de ningún tipo de *backup* de los datos almacenados de sus usuarios. • **R29**: No usa ningún tipo de antivirus para escanear los archivos almacenados en sus instalaciones. • **R30**: El proveedor indica que utiliza dispositivos de seguridad y tecnología que cumplen con las leyes y los estándares de la industria para proteger la información. Pero en su documentación no aparece cómo garantiza la integridad de la información almacenada.
Compartición	• **R10**: La compartición de archivos y carpetas se realiza a través de enlaces. La restricción de acceso a un recurso se realiza mediante la asignación de una contraseña, quien la posea tendrá acceso al recurso. Sólo su propietario puede asignar y modificar la contraseña. • **R11**: No permite la indexación de los archivos por motores de búsqueda. • **R12**: Los usuarios tienen acceso a un listado de recursos compartidos. • **R14**: El proveedor indica claramente los métodos de compartición.
Borrado	• **R19**: Sincronización de la eliminación de archivos entre todos los dispositivos conectados a la cuenta. • **R20**: No ha podido determinarse si se sobrescribe el espacio que ocupaban los datos borrados al ser eliminados definitivamente. • **R21**: Los archivos eliminados se guardan en la papelera de la cuenta del usuario hasta que se eliminan definitivamente pasados 60 días. Su propietario no puede decidir cuándo limpiar la papelera. Existen por tanto un periodo de retención después del borrado.
Cumplimiento de la legislación	• **R26**: Suecia forma parte de la UE y cumple con sus leyes sobre protección de datos, vigentes también en España.
Gestión de dispositivos	
Gestión multidispositivo	• **R16**: No existe listado de dispositivos registrados con una cuenta de usuario. • **R17**: El usuario no puede activar ni desactivar ninguno de sus dispositivos manualmente. • **R18**: El usuario no puede seleccionar el nombre de sus dispositivos asociados con su cuenta.
Actualización del software cliente	• **R22**: El software de los clientes puede actualizarse de forma automática o a instancias del usuario. • **R23**: No se han encontrados registros de actualizaciones.

TABLA 7 – CUMPLIMIENTO DE LOS REQUISITOS POR PARTE DE CLOUDME

6.5.3 Google Drive

Google Drive (https://drive.google.com) es uno de los principales productos de almacenamiento en la nube, que viene de la mano de uno de los principales proveedores de servicios Internet del planeta como es Google [59], cuya sede social está ubicada en Mountain View, California, EE.UU. El producto cuenta con la versión personal, objeto de este análisis, y la versión llamada Google Drive for Work.

Google Drive ofrece almacenamiento gratuito en la nube con capacidad de 15GB por cuenta, que comparte con el servicio de correo de Google Gmail y Google Fotos. Un usuario puede comprar almacenamiento extra de 100GB a 1,99$ al mes, 1TB a 9,99$ mensuales, 10TB a 99,99$ al mes, 20TB a 199,99$ mensuales o 30TB a 299,99$ al mes [50].

Según su documentación, permite gestionar los archivos de sus usuarios desde aplicaciones clientes instaladas en diferentes dispositivos conectados a Internet:

- Ordenadores personales con Microsoft Windows o Mac OS X.
- Dispositivos móviles con Android o iOS.

En este estudio, se analizará el cumplimiento de los requisitos para la consola *web* y el cliente de Windows, puesto que no existe ninguna versión oficial para Linux [50], para la versión personal de Google Drive.

Una de sus desventajas, que pueden hacer dudar a la hora de escogerlo como almacenamiento para nuestra información en la nube, es el hecho de que la Agencia Española de Protección de Datos (AEPD) no incluya a EE.UU. como país con un nivel adecuado de protección de datos personales y por tanto compatible con las leyes españolas y de la Unión Europea. Aunque, según la documentación de Google, la gran mayoría de sus servicios, entre los que se encuentra Google Drive, cuentan con la certificación ISO/IEC27001:2013 y con los sellos de garantía SOC1, SOC2 y SOC3 [57], que aseguran que cumple, entre otros, con los controles implantados para garantizar la confidencialidad, integridad y disponibilidad de la información.

6.5.3.1 Comunicaciones

6.5.3.1.1 Conexión

En las pruebas realizadas, Google Drive ha utilizado el protocolo seguro TLS, versiones 1.1 y 1.2, para **asegurar sus comunicaciones** entre los clientes y sus servidores. En algunas de las pruebas se han establecido diferentes conexiones seguras con las dos versiones indistintamente, aunque se usara el mismo cliente Windows, con el mismo Sistema Operativo y el mismo servidor, tal y como se muestra en la Figura 44. En todos los procesos de negociación de claves, el cliente Windows ha presentado las suites de la Figura 45, dependiendo de la versión del protocolo con la que se ha establecido la conexión. Los servidores de Google Drive han escogido las siguientes **suites de cifrado**, como puede verse en la Figura 46, las cuales se describen en el Anexo A:

- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA para TLS 1.1.
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 para TLS 1.2.

Con lo visto hasta ahora, puede decirse que cumple con el requisito **R1** al proporcionar **confidencialidad** e **integridad en las comunicaciones** [53]. Por otro lado, también se cumple el requisito **R3**, ya que el **servidor se autentica** ante los clientes presentando su certificado digital, que depende del proceso que se esté realizando en cada momento (autenticación, transmisión de

archivos, etc.). En la Figura 47 se muestra parte del certificado del servidor durante la subida de un archivo por parte del cliente Windows.

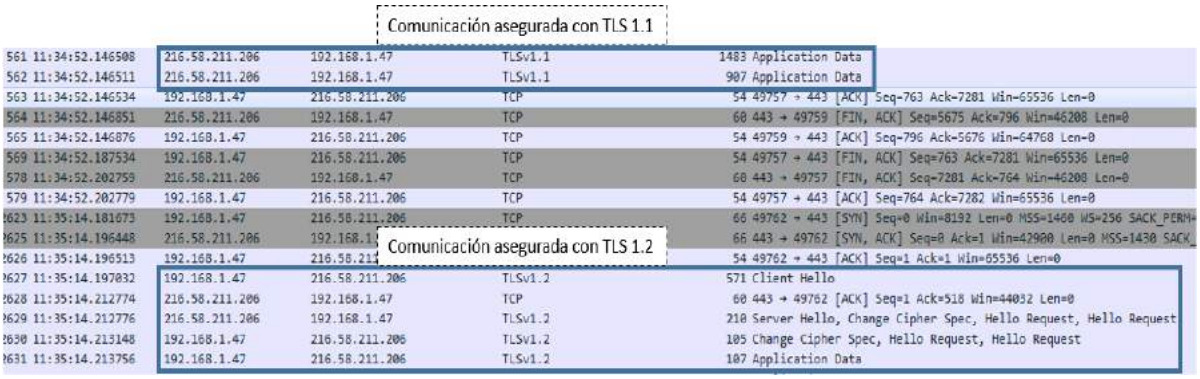


FIGURA 44 – EL MISMO CLIENTE WINDOWS, CON EL MISMO SISTEMA OPERATIVO Y SERVIDOR DE GOOGLE DRIVE UTILIZA VERSIONES DIFERENTES DEL PROTOCOLO TLS

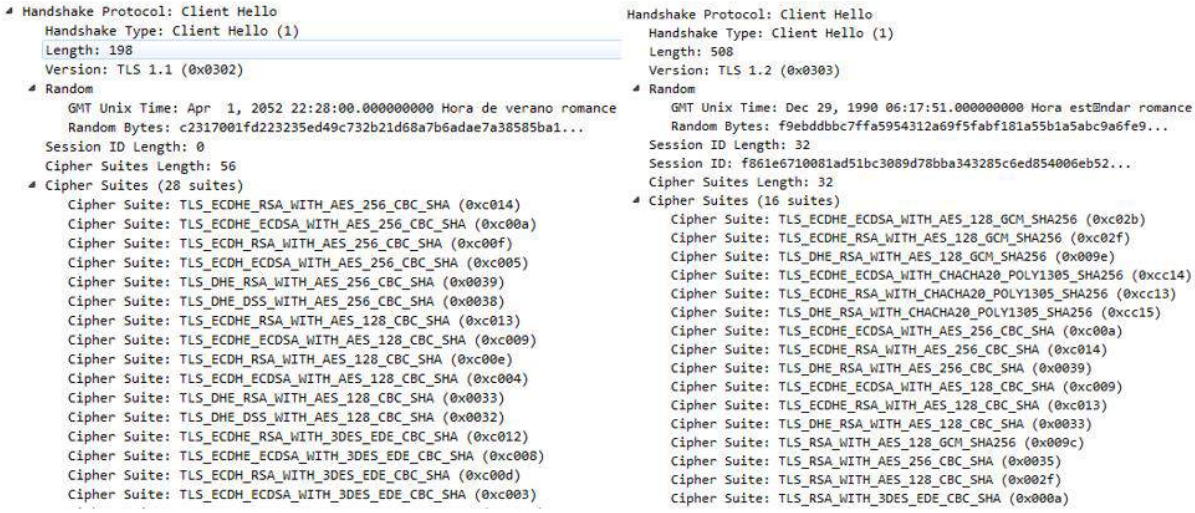


FIGURA 45 – SUITES DE CIFRADO PRESENTADAS POR EL MISMO CLIENTE WINDOWS SEGÚN LA VERSIÓN DEL PROTOCOLO TLS CON EL QUE SE REALIZA LA CONEXIÓN SEGURA

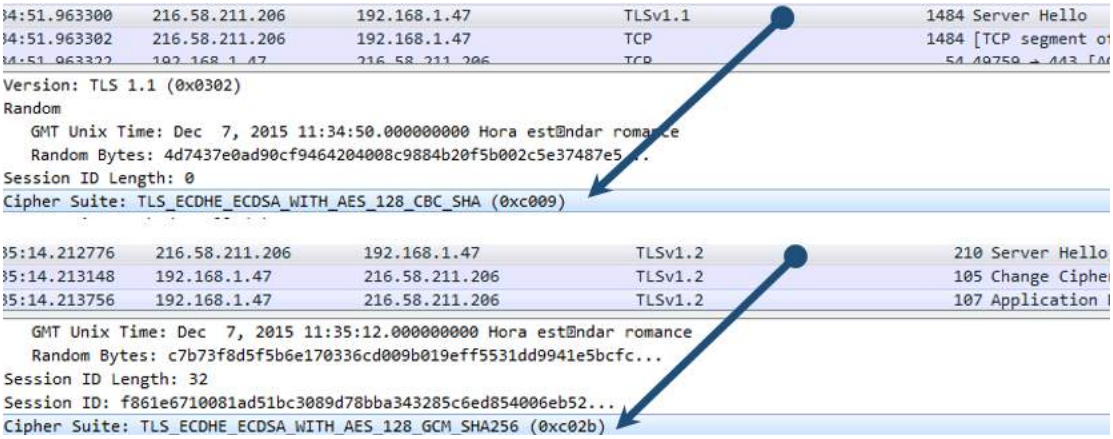


FIGURA 46 – SUITES DE CIFRADO ESCOGIDAS POR EL MISMO SERVIDOR CON EL MISMO CLIENTE WINDOWS Y SISTEMA OPERATIVO

FIGURA 47 – CERTIFICADO DEL SERVIDOR DE GOOGLE USADO DURANTE LA SUBIDA DE UN ARCHIVO

6.5.3.1.2 Registro

La **creación de una cuenta** en Google Drive debe realizarse a través de su página *web* de registro en Google. La cuenta podrá usarse para acceder a los diferentes servicios ofrecidos por Google. El formulario de registro requiere **recolectar** la siguiente **información** del usuario (ver Figura 48): nombre y apellidos, nombre de usuario (entre 6 y 30 caracteres), contraseña, repetición de contraseña, fecha de nacimiento, sexo, teléfono móvil (opcional), cuenta de correo electrónico actual (opcional y puede no ser de Google), un *captcha* para demostrar que no es un robot (opcional si el usuario desea omitirlo) y el país en el que supuestamente se encuentra el usuario. Al pulsar sobre el botón "Siguiente paso" aparecen las condiciones de uso, que deben aceptarse para poder seguir con el registro, y se solicita un número de móvil para verificar y finalizar la **activación** de la cuenta, a través de un código enviado por SMS o llamada de voz, cumpliendo así con el requisito **R7**. Con esto, puede decirse que la **recolección de información** es escueta, con lo que cumple con el requisito **R6**. Una vez finalizado el proceso de registro, el proveedor envía un correo electrónico confirmando su creación.

Debe destacarse que la **contraseña**, a pesar de enviarse a través de una conexión segura TLS, es recibida por los servidores de Google Drive sin procesar por una función *hash* o similar, con lo cual estos servidores tendrán acceso a la contraseña en claro, como puede verse en la captura de la Figura 49. Esto implica que tanto el personal interno del proveedor como un atacante, que comprometiera la seguridad de sus servidores, podrían tener **acceso a las contraseñas** de las cuentas de usuarios nuevos.

El registro de Google no está protegido contra la **enumeración de usuarios** existentes, es decir, no cumple con el requisito **R8**. Durante la etapa de registro, el formulario da pistas de los nombres de usuario disponibles y cuáles se encuentran dados de alta. Podría realizarse una lista de usuarios existentes de Google, para posteriormente lanzar un ataque contra sus cuentas. El formulario de registro, para averiguar si un nombre de usuario ya existe o está disponible, lanza una petición REST al servidor de Google, cuando el cursor sale del foco del campo de entrada del nombre de usuario, que responde si el nombre es válido (disponible) o no (ocupado), con la siguiente URL:

```
https://accounts.google.com/InputValidator?resource=SignUp
```

La información enviada en la petición es una estructura JSON como la que sigue:

```
{"input01":{"Input":"GmailAddress","GmailAddress":"<nombre
usuario>","FirstName":"","LastName":""},"Locale":"es"}
```

Con esta información, un atacante podría crear un programa sencillo que lanzara peticiones al proveedor, para averiguar si una serie de usuarios existen o bien están disponibles. En la Figura 50 se muestra el ejemplo de una petición lanzada con la aplicación SoapUI [56]. Puede verse en la imagen la petición (izquierda) y el resultado obtenido (derecha), que indica que el usuario no está disponible con el valor "*Valid": "false*".

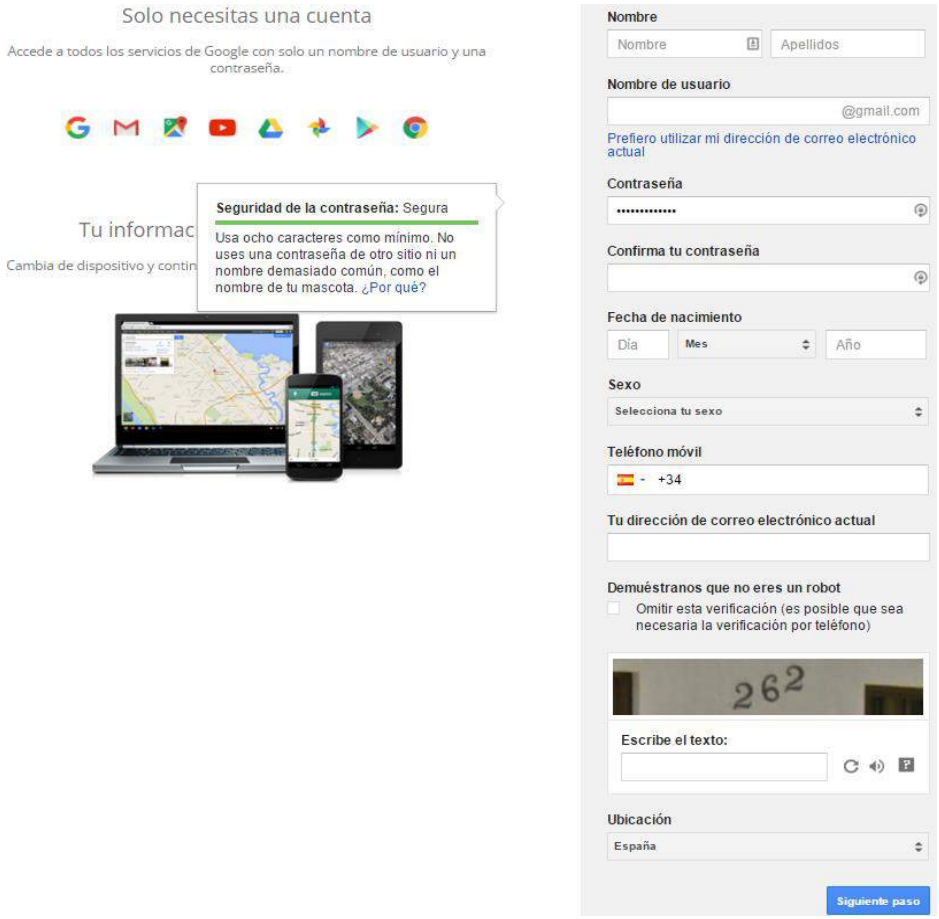


FIGURA 48 – FORMULARIO DE REGISTRO DE GOOGLE

FIGURA 49 – CAPTURA CON ZAP DE LA PETICIÓN DE REGISTRO EN GOOGLE

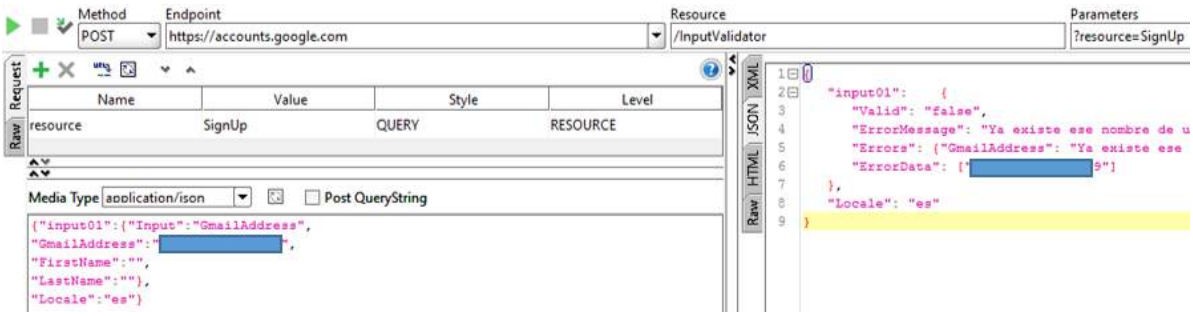


FIGURA 50 – PETICIÓN REST LANZADA DESDE SOAPUI PARA CONOCER LA EXISTENCIA O DISPONIBILIDAD DE UN NOMBRE DE USUARIO EN GOOGLE

En cuanto a la **selección de la contraseña**, ésta debe tener una longitud de entre 8 y 100 caracteres. Sólo admite caracteres del código US-ASCII. Durante su creación, el formulario de registro va informando sobre su calidad, indicando si es *poco segura*, *aceptable*, *suficiente* o *segura*, a medida que se va escribiendo, en orden ascendente de menos a más segura, rechazándose si es *poco segura*. **Permite** la creación de contraseñas con un solo tipo de carácter, con repeticiones de más de dos caracteres iguales (por ejemplo, *111MiPassword*) o con el número de móvil introducido en el formulario. **No permite** la creación de contraseñas iguales al nombre del usuario, que contengan un único carácter (por ejemplo, *aaaaaaaaaa*) o que sean palabras comunes como *password* o *google*. Solicita siempre la confirmación de la contraseña introducida. Sin embargo, aunque cumple con muchas de las características propuestas por OWASP en [48], no lo hace con algunas importantes como la longitud mínima de la contraseña, la posibilidad de introducir información personal del usuario o secuencias de caracteres repetidos. Por tanto, puede concluirse que no cumple con el requisito **R2**.

6.5.3.1.3 Login

La **autenticación básica** es de tipo usuario y contraseña para la consola web. Por otro lado, en el cliente Windows se crea un *token* de acceso de tipo *OAuth2* para el usuario de la cuenta a la que se conecta [54]. De esta forma, no es necesario introducir el nombre de usuario y contraseña para conectarse, excepto la primera vez. Este *token* caduca periódicamente y debe actualizarse, usando para este fin un *token* llamado de refresco. Ambos *tokens* se obtienen inicialmente durante el proceso de autorización al iniciarse el cliente Windows [54], como puede verse en la captura de la Figura 51. Puede concluirse, por tanto, que cumple con el requisito **R4**, ya que existe autenticación por parte del usuario en todos los casos.


```
{
  "access_token" : "ya29.RAJ2o-wyKr5bdwPy0BftagJkDCrERiURjKbUqPdsJWWDQiQBOoQePn2E2r4r6GO_i2YP",
  "token_type" : "Bearer",
  "expires_in" : 3600,
  "refresh_token" : "1/p-JnUOT-DsoS6pfQZ4AJObp9kapwY4opm4duAh4yx_w"
}
```


FIGURA 51 - CAPTURA ZAP CON LOS *TOKENS* DE ACCESO Y REFRESCO

Google permite configurar la **autenticación multifactor** para todos sus servicios, entre ellos Google Drive [50], desde la página *web* del usuario. Para autenticarse, el usuario debe introducir su nombre de usuario, contraseña y un código de verificación único, que puede obtenerse de cuatro formas distintas: mediante el envío por parte de Google del código en un SMS al móvil indicado, realizando una llamada de voz en la que Google indica el código, de una lista de códigos fijos que el usuario puede usar cuando no dispone de móvil o mediante una aplicación móvil que debe descargarse el usuario y calcula nuevos códigos de verificación cada 60 segundos (ver ejemplo de la Figura 52). Si se quiere autenticar desde el cliente Windows, es suficiente con introducir el código de verificación

una sola vez para que se cree el *token OAuth2*. Por tanto, puede concluirse que cumple con el requisito **R5** al permitir la autenticación multifactor.

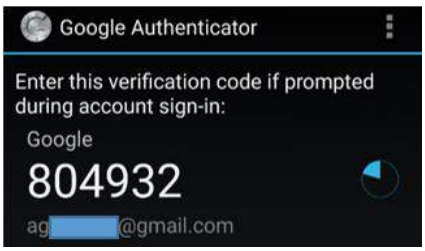


FIGURA 52 - APLICACIÓN ANDROID PARA EL CÁLCULO DE CÓDIGOS DE VERIFICACIÓN DE GOOGLE

Como en el de registro, el formulario de *login* de la consola *web* da pistas sobre los usuarios existentes, es decir, permite **enumeración de usuarios**. Si se introduce uno inexistente, indica que no es un usuario válido. En cambio, si se introduce uno existente con la contraseña errónea, se indica que el usuario o la contraseña son erróneos, tal y como puede verse en la Figura 53. Al igual que en el caso del registro, puede concluirse que no cumple con el requisito **R8** al permitir enumerar usuarios existentes.

FIGURA 53 – ENUMERACIÓN DE USUARIO EN EL FORMULARIO DE *LOGIN* DEL CLIENTE *WEB*

Todas las credenciales se envían a través de una conexión segura TLS. Como ocurre con el proceso de registro, la contraseña no se procesa previamente por ninguna función *hash* o similar, por lo que los servidores tendrán acceso a la contraseña en claro, con lo que un atacante que comprometa los servidores de Google o personal interno malicioso podrá tener acceso a las contraseñas en claro de las cuentas de sus usuarios [18]. En la Figura 54 puede verse una captura del proceso de *login*.

FIGURA 54 – CAPTURA CON ZAP DURANTE LA PETICIÓN DE *LOGIN* EN GOOGLE DRIVE

6.5.3.2 Tratamiento de la información

6.5.3.2.1 Transmisión de archivos

Toda la transmisión de archivos entre los servidores de Google Drive y sus clientes se realiza a través de una conexión segura TLS, con lo que la transmisión queda asegurada. Google Drive **no cifra los archivos** en el lado cliente antes de subirlos a sus servidores [16], tal y como confirman las pruebas realizadas durante el análisis, concluyendo que no cumple con el requisito **R9**. En la Figura 55 se muestra la captura del contenido de un archivo de texto subido a Google Drive desde el cliente Windows y en la Figura 56 la captura de un archivo subido desde la consola *web* y descargado posteriormente por el cliente Windows. Esto implica que el personal interno o un atacante, que comprometiese la seguridad de los servidores de Google Drive, podrían tener acceso a la información que llega a sus instalaciones [18]; poniendo en peligro el cumplimiento del requisito **R10**, puesto que el atacante podría tener **acceso al contenido** de los archivos **sin autorización** para ello.

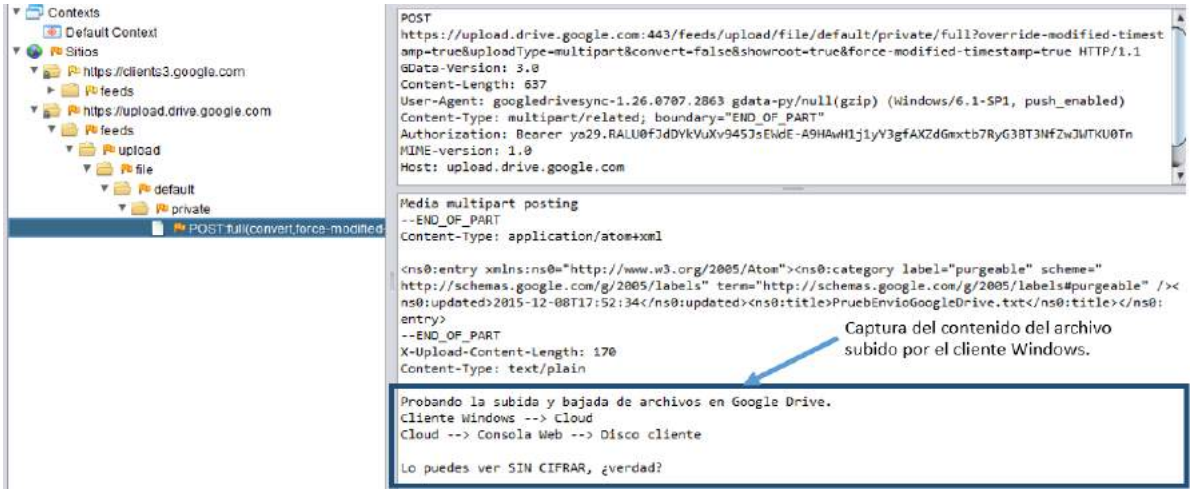


FIGURA 55 – CAPTURA CON ZAP DE LA SUBIDA DE UN ARCHIVO DESDE EL CLIENTE WINDOWS

FIGURA 56 –DESCARGA POR EL CLIENTE WINDOWS DE UN ARCHIVO SUBIDO CON LA CONSOLA *WEB*

En su documentación [57], Google Drive no menciona en ningún momento el uso del **proceso de deduplicación** en su servicio. Para revisar el cumplimiento del requisito **R15**, se han realizado pruebas en las que se ha comprobado que no realiza la deduplicación en cliente; siempre sube los archivos completos, aunque su contenido sea exactamente el mismo a uno ya existente, bien en la misma cuenta de usuario o en la de otro.

En dichas pruebas, se ha subido el mismo archivo de 200MB[4] dos veces (con nombres diferentes) a la misma cuenta X de Google Drive por un lado y una más a otra cuenta diferente Y. En todos los casos, como puede verse en los bytes transmitidos de la Figura 57, Figura 58 y Figura 59, el archivo se sube completo al servidor, con lo que queda **descartada la deduplicación en el lado cliente**. No se ha podido averiguar si realiza deduplicación en el servidor, con lo que, a tenor de la dificultad de encontrar documentación al respecto y por las búsquedas de información realizadas en Internet, donde se dan consejos de cómo borrar archivos duplicados en Google Drive, puede deducirse que actualmente no se realiza deduplicación de datos para almacenar la información en sus servidores. Por tanto, puede concluirse que cumple con el requisito **R15**.

Address A	Address B	Bytes	Bytes A→B	Bytes A←B	Packets	Packets A→B	Packets A←B
192.168.1.15	216.58.211.239	228 173 230	223 056 357	5 116 873	226 084	150 833	75 251
176.106.54.54	192.168.1.15	51 600	26 958	24 642	147	73	74
192.168.1.15	192.168.1.143	46 661	294	46 367	179	3	176
64.233.167.189	192.168.1.15	41 528	14 648	26 880	162	73	89

FIGURA 57 – CAPTURA DE LA SUBIDA DEL PRIMER ARCHIVO DE X DESDE UN CLIENTE WINDOWS

Address A	Address B	Bytes	Bytes A→B	Bytes A←B	Packets	Packets A→B	Packets A←B
192.168.1.15	216.58.211.239	150 527 800	147 033 084	3 494 716	150 557	99 437	51 120
192.168.1.15	216.58.210.143	79 929 028	78 070 145	1 858 883	79 123	52 786	26 337
176.106.54.54	192.168.1.15	87 202	45 825	41 377	243	120	123
192.168.1.15	192.168.1.143	85 005	392	84 613	326	4	322

FIGURA 58 - CAPTURA DE LA SUBIDA DEL SEGUNDO ARCHIVO DE X DESDE EL MISMO CLIENTE

Address A	Address B	Bytes	Bytes A → B	Bytes B → A	Packets	Packets A → B	Packets B → A
192.168.1.44	216.58.210.143	205 M	201 M	4123 k	81 254	14350	66904
192.168.1.42	192.168.1.44	9862	8741	1121	30	17	13
192.168.1.44	216.58.211.238	8771	1615	7156	22	10	12
192.168.1.15	192.168.1.44	4497	2327	2170	38	23	15

FIGURA 59 – CAPTURA DE LA SUBIDA DEL ARCHIVO DE Y DESDE OTRO CLIENTE WINDOWS

En cuanto a la **integridad de los archivos transmitidos**, el cliente Windows almacena en una BDD SQLite (llamada *snapshot.db*) el *checksum* MD5 de todos los archivos que sincroniza. En el **proceso de subida** de un archivo, el cliente Windows recibe el *checksum* MD5 del archivo, como parte de la respuesta del servidor, tal y como puede verse en la respuesta capturada con ZAP de la Figura 60. Hasta donde ha podido analizarse, podría estar comparando la respuesta del servidor con el valor del *checksum*, que se habría calculado antes de realizar la subida, con el fin de verificar su integridad. En el **proceso de descarga**, el cliente Windows recibe el archivo junto con su *checksum* MD5, como puede verse en la captura con ZAP de la Figura 61. Esto último podría estar indicando que el cliente realiza una comprobación del *checksum* recibido, contra el que habría calculado al recibir el archivo, para verificar su integridad.

En conclusión, la verificación de la integridad de la información transmitida se estaría llevando a cabo en el lado del cliente Windows. Pero al no ser posible probarlo con precisión, puesto que no se tiene acceso al código fuente ni se ha encontrado documentación que lo explique, no puede confirmarse el cumplimiento del requisito **R28**.

[4] Los 200MB permitirán distinguir claramente los bytes correspondientes a las capturas con *Wireshark*.

```
<entry xmlns='http://www.w3.org/2005/Atom' xmlns:batch='http://schemas.google.com/gdata/bat
'http://schemas.google.com/docs/2007' gd:etag='&quot;ABIESEhCFSt7ImBl&quot;'>
    <id>https://upload.drive.google.com/feeds/id/file%3A0B-q2grLgfKE4Y09ScWNaeFRLNTA</id>
    ...
    <title>SuboFichero4.txt</title>
    ...
    <author>
        <name>seguridadmictic</name>
        <email>seguridadmictic@gmail.com</email>
    </author>
    <gd:resourceId>file:0B-q2grLgfKE4Y09ScWNaeFRLNTA</gd:resourceId>
    ...
    <docs:md5Checksum>3201e90f582281cb5a0bca82d30713f9</docs:md5Checksum>
    <docs:filename>SuboFichero4.txt</docs:filename>
    ...
</entry>
```

FIGURA 60 – RESPUESTA DEL SERVIDOR DE GOOGLE DRIVE ANTE LA SUBIDA DE UN ARCHIVO NUEVO

```
HTTP/1.1 206 Partial Content
X-GUploader-UploadID: AEnB2UrSEUTLdUo5jUH3_JklvI9-nsP3kfQc
Content-Type: audio/mpeg
Date: Sun, 13 Dec 2015 12:05:40 GMT
Content-MD5: 3dIDPYTKJ/jrh/gBVUgVFg==
Unzipped-Content-MD5: 3dIDPYTKJ/jrh/gBVUgVFg==
```

FIGURA 61 –RESPUESTA DE DESCARGA EN LA QUE SE MUESTRA EL *CHECKSUM* DEL ARCHIVO

6.5.3.2.2 Almacenamiento

En cuanto al uso de **sistemas antivirus**, no está muy claro cuál utiliza para escanear los archivos almacenados por sus usuarios. Realizando pruebas, se llega a la conclusión de que permite sincronizar archivos infectados entre aplicaciones clientes, como en el ejemplo de la Figura 62, en el que se ha subido el archivo desde la consola *web* y se ha sincronizado con el cliente Windows. Sin embargo, si un usuario pretende descargar un archivo infectado desde la consola *web*, con tamaño de hasta unos 25MB, se le advierte de esta circunstancia, como en el ejemplo de la Figura 63. Podemos concluir que el requisito **R29** se cumple en parte, y sólo es posible un control del *malware* si el usuario pretende descargarse un archivo no muy grande desde la *web*.

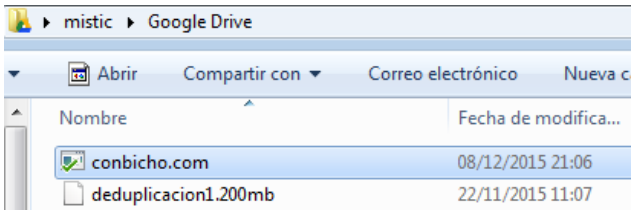


FIGURA 62 – ARCHIVO INFECTADO Y SINCRONIZADO ENTRE LOS CLIENTES DE GOOGLE DRIVE

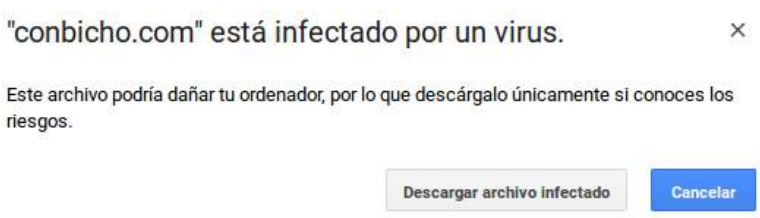


FIGURA 63 – ADVERTENCIA EN LA CONSOLA *WEB* DE ARCHIVO INFECTADO

En cuanto al **cifrado de datos en el lado cliente**, como ya se resaltó en el apartado anterior, Google Drive **no cifra** los archivos en sus clientes, con lo que no cumple con los requisitos **R9** y **R10**.

En cuanto a la **localización de sus servidores**, Google señala en su documentación [55] que sus centros de datos se encuentran distribuidos en diferentes puntos del planeta: EE.UU. y Chile en América; Hong Kong, Singapur y Taiwán en Asia y Finlandia, Bélgica e Irlanda en Europa. Por tanto, cumple con el requisito **R24** al proporcionar información sobre dónde almacena la información de sus usuarios. Sin embargo, en las pruebas realizadas, las diferentes IP de Google se han localizado en EE.UU., como puede verse en el resultado de la consulta de la Figura 64, realizada contra el servicio de localización IP http://www.ipligence.com/iplocation. Sin embargo, Google no indica si los usuarios pueden **escoger la localización** de sus datos, con lo que estaría incumpliendo el requisito **R25**.

Google indica en su documentación [55] que realiza copias de seguridad de todos los datos de sus usuarios, con lo que estaría cumpliendo así con el requisito **R27**. Por otro lado, en la misma documentación, se indica que realiza el mantenimiento necesario para asegurar la disponibilidad e integridad de la información, por tanto, ateniéndonos a sus certificaciones, puede decirse que cumple también con el requisito **R30**.

IP ADDRESS	CONTINENT	FLAG	COUNTRY	REGION	CITY
216.58.211.239	North America		United States	California	Mountain View
216.58.210.143	North America		United States	California	Mountain View
216.58.211.238	North America		United States	California	Mountain View
216.58.210.170	North America		United States	California	Mountain View
216.58.211.205	North America		United States	California	Mountain View
216.58.210.163	North America		United States	California	Mountain View
216.58.210.196	North America		United States	California	Mountain View
216.58.216.207	North America		United States	California	Mountain View
74.125.140.125	North America		United States	California	Mountain View
74.125.71.189	North America		United States	California	Mountain View
74.125.206.189	North America		United States	California	Mountain View

FIGURA 64 – LOCALIZACIÓN DE LAS IP DE GOOGLE EN LAS PRUEBAS REALIZADAS

6.5.3.2.3 Compartición

La documentación y las posibilidades de compartición de recursos en Google Drive es muy amplia, con lo que para profundizar en su funcionamiento es aconsejable acceder a su página de soporte [57], donde se **detallan los métodos de compartición** que provee, cumpliendo así con el requisito **R14**. En este apartado, se intenta dar una pincelada de las principales características, de relevancia para este análisis.

Google Drive permite **compartir archivos y carpetas** con otros usuarios [57]. Siempre que se comparte un recurso, se crea un enlace que puede abrirse desde cualquier navegador *web*. Como puede verse en la Figura 65, el propietario puede decidir si el recurso compartido:

- Se hace **público en la *web***, para que cualquiera que encuentre su enlace pueda acceder a su contenido en modo de **sólo lectura**.
- Puede ser **leído**, pero no modificado, por cualquiera que haya **recibido su enlace**.
- Puede ser **leído**, **modificado** o **comentado** sólo por ciertos usuarios, con los **permisos** de acceso que les sean otorgados, como veremos más adelante.

Si se comparte una carpeta, quien tenga acceso a ella tendrá acceso a su contenido, para el que podrán definirse permisos de forma individual, de tal manera que los usuarios podrán acceder a diferentes partes del contenido con permisos diferentes.

En cuanto a la **restricción de acceso** a los recursos, pueden definirse diferentes permisos para los distintos usuarios a los que se le dé acceso. Estos permisos son cuatro y se identifican como (ver Figura 66): *es propietario, puede editar, puede comentar* y *puede ver*. Sólo el propietario puede otorgar y denegar permisos, permitiendo modificar los permisos de los archivos y carpetas de forma individual, en contraposición a los productos analizados anteriormente. Por tanto, puede decirse que cumple con el requisito **R10**. Sin embargo, debe tenerse en cuenta que en las condiciones de servicio de Google [50] se indica textualmente que "*Podemos revisar el contenido para determinar si es ilegal o infringe nuestras políticas, y eliminarlo o negarnos a publicarlo si tenemos razones suficientes para considerar que infringe nuestras políticas o la ley*", es decir, el propio proveedor se atribuye para sí el permiso de acceder al contenido en cualquier momento, permiso que concede el usuario al aceptar las condiciones de uso, con lo que seguiría cumpliendo con el requisito **R10**.

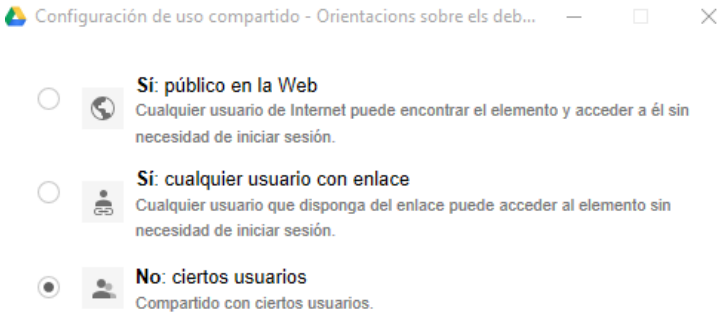


FIGURA 65 – CONFIGURACIÓN DE USO COMPARTIDO EN GOOGLE DRIVE

FIGURA 66 – COMPARTICIÓN DE RECURSOS EN GOOGLE DRIVE

Según la política de privacidad de Google, muchos de sus servicios permiten compartir información con otros usuarios, pudiendo ser **indexada por motores de búsqueda** si se comparte públicamente [50]. Al aceptar las condiciones de servicio de Google, los usuarios también aceptan su política de privacidad, con lo que consienten en que sus datos compartidos de forma pública sean indexados por motores de búsqueda. En este sentido, Google estaría cumpliendo con el requisito **R11**, ya que el usuario siempre da su consentimiento para crear una nueva cuenta (o se queda sin ella). Pero si se comparten de forma privada, si nos atenemos a las pruebas realizadas, también estaría cumpliendo con **R11**, ya que no ha sido posible encontrar ningún recurso compartido desde ningún motor de búsqueda de Google, Bing o Yahoo.

Un usuario de Google Drive puede acceder al **listado de los recursos** que tiene **compartidos** con otros usuarios. En la Figura 67 pueden verse los archivos y carpetas compartidos, marcados con símbolos de personas (2 para los archivos y 1 para las carpetas). Por consiguiente, puede concluirse que cumple con el requisito **R12**.

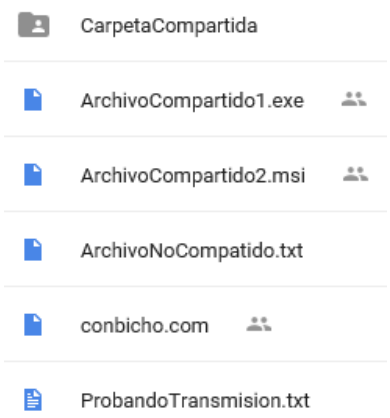


FIGURA 67 - LISTADO DE ARCHIVOS Y CARPETAS DONDE SE MARCAN LOS COMPARTIDOS

6.5.3.2.4 Borrado

Cualquier archivo o carpeta que elimina un usuario queda almacenado permanentemente en la papelera de su cuenta, hasta que decide eliminarlo de forma definitiva, independientemente de si se borra en la consola *web* o desde cualquiera de los clientes de Google Drive. El borrado de un archivo desde un cliente implica su eliminación en el resto de dispositivos conectados a la cuenta del usuario [57], extremo que se ha comprobado con la realización de pruebas. Por tanto, puede concluirse que cumple con el requisito **R19**, al **sincronizarse el borrado** en todos los dispositivos.

En la documentación de Google Drive, no ha sido posible encontrar qué ocurre con los datos y su **espacio en disco** cuando se eliminan definitivamente de la papelera. Además, en caso de que un usuario dé de baja su cuenta en Google, la da de baja de todos los servicios asociados a la misma, entre ellos Google Drive. En este último caso, en su documentación indica textualmente que "*ya no podrás usar lo siguiente… Datos asociados a tu cuenta, incluidos los correos electrónicos, las fotos y los registros de transacciones.*" [57], pero no habla de eliminar la información que el usuario tenga almacenada, sólo de que su propietario pierde el acceso a la misma. Con todo esto y la documentación existente, no puede determinarse el cumplimiento de los requisitos **R20** y **R21**.

6.5.3.2.5 Cumplimiento de la legislación

Google Drive, tal y como se indica en su documentación [50], está sujeta a las leyes del estado de California en EE.UU. Desde julio de 2000 hasta octubre de 2015, estuvo en vigor el Marco de Puerto Seguro, entre la Unión Europea y EE.UU., con el fin de salvar las diferencias entre las legislaciones

de ambas partes en materia de protección de datos personales. Esto permitía a las empresas europeas transmitir y almacenar datos personales de forma legal en aquellos proveedores de EE.UU. adheridos al Marco de Puerto Seguro [27], siendo Google uno de estos proveedores [50]. Sin embargo, en sentencia del 6 de octubre de 2015, la Corte de Justicia de la Unión Europea declaró inválido el Marco de Puerto Seguro [27]. Por tanto, EE.UU. deja de ser considerado como un país con un nivel adecuado de protección datos personales para la AEPD. Atendiendo a lo indicado por la AEPD, se considera que Google Drive no cumple con el requisito **R26**.

6.5.3.3 Gestión de dispositivos cliente

6.5.3.3.1 Multidispositivo

Google Drive permite trabajar con distintos dispositivos y sistemas operativos. Sin embargo, un usuario sólo puede ver los dispositivos con los que se ha conectado últimamente desde un **navegador *web*** a cualquier servicio de Google, pero **no puede saberse si lo ha hecho desde las aplicaciones cliente de Google Drive** [62]. Por tanto, puede concluirse que no cumple con los requisitos **R16**, **R17** y **R18**.

6.5.3.3.2 Actualización del software de los clientes

Google indica en sus condiciones de servicio [50] que cuando un servicio incluye software que se puede descargar, éste se **actualizará automáticamente** en el dispositivo del usuario cuando haya nuevas versiones disponibles. En el cliente de Windows no hay posibilidad de que el usuario pueda indicar si las actualizaciones deben ser automáticas o cuando éste lo decida. Por tanto, teniendo en cuenta lo que se indica en [50], se concluye que existen actualizaciones sólo automáticas del software, cumpliendo sólo en parte el requisito **R22**.

En cuanto al **registro de cambios**, no ha sido posible encontrar en la documentación de Google nada que indique que se lleva un control de cambios del software cliente. Tampoco ha sido posible realizar pruebas en este sentido, puesto que no se ha liberado ninguna versión nueva de los clientes durante el análisis. Con esto, no puede determinarse si se cumple con el requisito **R23**.

6.5.3.4 Conclusiones

En la Tabla 8 se resume el cumplimiento o no de los diferentes requisitos. La principal conclusión que puede obtenerse es que Google Drive puede presentar problemas de seguridad en el tratamiento de la información; aunque presenta puntos fuertes como la implementación de la compartición de archivos y carpetas. Entre sus problemas, puede destacarse:

- La amenaza de **violación de los datos** de sus usuarios, al no cifrarse la información enviada por las aplicaciones clientes hacia sus servidores, ya sea por el ataque de un empleado malicioso o a través de otro atacante que sea capaz de comprometer los servidores de Google Drive.
- El proceso de registro permite **enumerar** fácil y automáticamente a conjuntos importantes de sus usuarios.
- No cumple con la **legislación** de la Unión Europea, desde la invalidación del Marco de Puerto Seguro por parte de la justicia europea, en lo referente a protección de datos personales. El incumplimiento de la legislación de la UE puede acarrear graves sanciones económicas para el usuario del servicio de Google Drive.

Procesos	Cumplimiento de los requisitos
Comunicaciones	
Conexión	• **R1**: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA con protocolo seguro TLS versión 1.1. TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 con TLS 1.2.

Procesos	Cumplimiento de los requisitos
	• **R3**: Los servidores se autentican ante los clientes usando certificado digital dependiendo del proceso que se esté realizando en cada momento.
Registro	• **R2**: No utiliza contraseñas robustas según definición de OWASP. • **R6**: Recolección escueta de datos. • **R7**: Solicita activación de la cuenta de usuario a través de código enviado por SMS al móvil proporcionado. • **R8**: Permite enumeración de usuarios. • Los datos del registro se envían a través de TLS, pero la contraseña no se procesa con una función *hash* o similar, con lo que los servidores tienen acceso a su valor en claro.
Login	• **R4**: Autenticación básica de tipo usuario y contraseña. Creación de *token* OAuth2 para los clientes Windows. • **R5**: Soporta autenticación multifactor. • **R8**: Permite enumeración de usuarios. • Los datos del *login* se envían a través de TLS, pero la contraseña no se procesa con una función *hash* o similar, con lo que los servidores tienen acceso a su valor en claro.
Tratamiento de la información	
Transmisión de archivos	• **R9**: No cifra los archivos en el lado cliente antes de su envío a los servidores. Los servidores tienen acceso a su valor en claro. • **R15**: No usa deduplicación para almacenar los archivos. • **R28**: El cliente Windows siempre recibe por parte del servidor el *checksum* MD5 de los archivos que sube y descarga.
Almacenamiento	• **R9**: No cifra los archivos en el lado cliente. • **R10**: Al no cifrar los datos en el lado cliente, permite a los servidores tener acceso en claro de los archivos almacenados. • **R24**: Según su documentación, los datos de sus usuarios pueden almacenarse en diferentes localizaciones de América, Asia y Europa. • **R25**: Los usuarios no pueden seleccionar la localización de sus datos. • **R27**: En la documentación se informa de la realización de *backups* de los datos almacenados de sus usuarios. • **R29**: Usa un sistema de antivirus que escanea los archivos que se descargan desde su consola *web* y que ocupen hasta un máximo de 25MB. • **R30**: Su documentación indica que se realiza el mantenimiento necesario para asegurar la disponibilidad e integridad de los datos almacenados.
Compartición	• **R10**: La compartición de archivos y carpetas se realiza a través de enlaces. Permite restringir su acceso de forma individual a usuarios distintos con niveles de permisos diferentes. • **R11**: Según su documentación, permite la indexación de los archivos por motores de búsqueda si comparten públicamente a través de la *web*. En el resto de casos no se permite. • **R12**: Los usuarios tienen acceso a un listado de recursos compartidos. • **R14**: El proveedor indica claramente los métodos de compartición.
Borrado	• **R19**: Sincronización de la eliminación de archivos entre todos los dispositivos conectados a la cuenta. • **R20**: No ha podido determinarse si se sobrescribe el espacio que ocupaban los datos borrados al ser eliminados definitivamente. • **R21**: Los archivos eliminados se guardan en la papelera de la cuenta del usuario hasta que se eliminan definitivamente por parte del usuario. En su documentación se indica que cuando se da de baja una cuenta, su usuario simplemente deja de tener acceso a sus datos, sin especificar qué hace con ellos.
Cumplimiento de la legislación	• **R26**: La AEPD no considera que EE.UU., sede del proveedor, sea un país con un nivel adecuado de protección.

Procesos	Cumplimiento de los requisitos
Gestión de dispositivos	
Gestión multidispositivo	• **R16**: Existe listado de dispositivos registrados con una cuenta de usuario, que haya accedido desde una consola *web*, pero no desde cualquier otro tipo de cliente. • **R17**: El usuario no puede activar ni desactivar ninguno de sus dispositivos manualmente. • **R18**: El usuario no puede seleccionar el nombre de sus dispositivos asociados con su cuenta.
Actualización del software cliente	• **R22**: El software de los clientes puede actualizarse de forma automática o a instancias del usuario. • **R23**: No se han encontrados registros de actualizaciones.

TABLA 8 – CUMPLIMIENTO DE LOS REQUISITOS POR PARTE DE GOOGLE DRIVE

6.5.4 Comparativa entre productos

En la siguiente tabla se resumen, a modo de comparativa, las principales propiedades de los procesos analizados de los diferentes productos. Para detalles específicos debe consultarse la sección correspondiente.

Procesos	Productos	Propiedades
Comunicaciones		
Conexión	Yandex.Disk	TLS 1.2, con certificado digital con clave pública RSA.
	CloudMe	TLS 1.2, con certificado digital con clave pública RSA.
	Google Drive	TLS 1.1 y TLS 1.2, con certificado digital dependiendo del proceso que se esté realizando.
Registro	Yandex.Disk	Contraseñas no robustas y enviadas sin procesar por TLS. Activación de cuenta vía móvil si usuario proporciona número. Enumeración de usuarios.
	CloudMe	Contraseñas no robustas y enviadas sin procesar por TLS. Sin solicitud de activación de cuenta de usuario. Enumeración de usuarios.
	Google Drive	Contraseñas no robustas y enviadas sin procesar por TLS. Activación de cuenta vía móvil. Enumeración de usuarios.
Login	Yandex.Disk	Contraseñas enviadas sin procesar por TLS. Autenticación de tipo usuario/contraseña y *token* OAuth2 para clientes Windows y Linux. Autenticación multifactor.
	CloudMe	Contraseñas procesadas con función MD5 enviadas por TLS. Autenticación de tipo usuario/contraseña.
	Google Drive	Contraseñas enviadas sin procesar por TLS. Autenticación de tipo usuario/contraseña y *token* OAuth2 para clientes Windows. Autenticación multifactor.
Tratamiento de la información		
Transmisión de archivos	Yandex.Disk	Deduplicación *cliente – cross-user*. Archivos enviados por TLS y sin cifrar en el cliente. Calculo de *checksum* MD5 y *hash* SHA-256 de los archivos.
	CloudMe	No realiza deduplicación de archivos. Archivos enviados por TLS y sin cifrar en el cliente. Calculo de *checksum* MD5 de los archivos.
	Google Drive	No realiza deduplicación de archivos. Archivos enviados por TLS y sin cifrar en el cliente. Calculo de *checksum* MD5 de los archivos.

Procesos	Productos	Propiedades
Almacenamiento	Yandex.Disk	No se cifran los archivos en el cliente. No existe información sobre localización de almacenamiento. Escaneo antivirus para archivos de hasta 1GB.
	CloudMe	No se cifran los archivos en el cliente. Almacenamiento localizado en Suecia, según documentación. No se escanean archivos en busca de *malware*.
	Google Drive	No se cifran los archivos en el cliente. Almacenamiento localizado en América, Asia y Europa. Escaneo antivirus para archivos de hasta 25MB, descargados desde la consola *web*.
Compartición	Yandex.Disk	Enlaces no protegidos para archivos y carpetas. Enlaces protegidos para carpetas con usuario y contraseña. Diferentes niveles de permisos de acceso a las carpetas. Acceso a listado de recursos compartidos. No permite la indexación por motores de búsqueda.
	CloudMe	Enlaces no protegidos y protegidos mediante contraseña. Acceso a listado de recursos compartidos. No permite la indexación por motores de búsqueda.
	Google Drive	Enlaces no protegidos y protegidos con usuario y contraseña. Diferentes niveles de permisos de acceso a los recursos. Acceso a listado de recursos compartidos. No permite la indexación por motores de búsqueda para recursos no compartidos públicamente en la *web*.
Borrado	Yandex.Disk	El borrado de archivos se sincroniza entre todos los dispositivos asociados con la cuenta del usuario. Archivos eliminados en guardan en la papelera hasta que el usuario los elimina o pasen 30 días.
	CloudMe	El borrado de archivos se sincroniza entre todos los dispositivos asociados con la cuenta del usuario. Archivos eliminados en guardan en la papelera 60 días. El usuario no puede decidir eliminarlos definitivamente.
	Google Drive	El borrado de archivos se sincroniza entre todos los dispositivos asociados con la cuenta del usuario. Archivos eliminados en guardan en la papelera hasta que el usuario los elimina definitivamente. No se puede especificar qué ocurre al darse de baja una cuenta.
Cumplimiento de la legislación	Yandex.Disk	Rusia, país del proveedor, no se considera un país con un nivel adecuado de protección de datos personales.
	CloudMe	Cumple las leyes de la UE en cuanto a protección de datos personales.
	Google Drive	EE.UU., país del proveedor, no se considera un país con un nivel adecuado de protección de datos personales.
Gestión de dispositivos		
Gestión multidispositivo	Yandex.Disk	No existe listado de dispositivos registrados.
	CloudMe	No existe listado de dispositivos registrados.
	Google Drive	Existe un listado de dispositivos por cuenta de usuario, pero que han accedido a cualquier servicio de Google desde un navegador *web*.
Actualización del software cliente	Yandex.Disk	Actualizaciones automáticas y bajo demanda del software.
	CloudMe	Actualizaciones automáticas y bajo demanda del software.
	Google Drive	Actualizaciones automáticas y bajo demanda del software.

TABLA 9 – TABLA COMPARATIVA DEL CUMPLIMIENTO DE LOS REQUISITOS ANALIZADOS

6.5.5 Conclusiones del análisis

El resultado principal, que puede extraerse del análisis, es el hecho de que **ninguno** de los productos estudiados **cumple con todos los requisitos de seguridad**; a pesar de que sus proveedores afirman en su documentación, de forma más o menos extensa, que son plenamente conscientes de la importancia que tiene la seguridad de los datos de sus usuarios. Los requisitos que más incumplimiento presentan son los relacionados con el cifrado de datos, registro y *login* de usuarios y la gestión de dispositivos cliente.

Ante los resultados obtenidos, puede afirmarse que una de las amenazas más importantes a las que se enfrentan los proveedores y sus usuarios es la **violación de datos**. Esto es debido, principalmente, al incumplimiento de los requisitos de cifrado de datos en el lado del cliente, lo que provoca que la información sea enviada sin cifrar y pueda ser revelada en el lado del servidor. Sin embargo, todos los productos **aseguran sus comunicaciones** con el protocolo TLS, mitigando así el impacto que pudieran tener los ataques contra el transporte de datos.

En la **compartición** de datos, todos los productos presentan procesos diferentes, aunque tengan puntos en común, como la posibilidad de compartir archivos públicamente (fuente de problemas con la privacidad y revelación de datos). Dos de los productos permiten otorgar permisos de acceso por usuario y el tercero sólo asigna una contraseña al recurso, quien la obtiene puede acceder, perdiendo el control de los usuarios con los que realmente se comparte.

En cuanto al **registro de nuevos usuarios**, todos los productos presentan problemas comunes: permiten enumerar usuarios existentes; enviar datos de registro sin cifrar a los servidores del proveedor; elección de contraseñas poco robustas, que pueden acabar llevando a ataques exitosos de secuestro de cuentas o servicios y, en algún caso, permite crear nuevas cuentas de usuarios de forma masiva, lo que puede ser utilizado por un atacante para lanzar ataques de denegación de servicio contra el proveedor.

En lo referente al proceso de ***login***, éste incumple prácticamente los mismos requisitos que el registro. Sólo se ha encontrado un producto que cifra la contraseña antes de enviarla al servidor y que no permite la enumeración de usuarios. Sin embargo, dos de los tres productos permiten el uso de autenticación multifactor, que añade seguridad extra al proceso de *login*.

En cuanto a la **gestión de dispositivos** del usuario, ninguno de los productos permite llevar una gestión acorde con las necesidades planteadas. Cuando los usuarios pierden alguno un dispositivo (se lo roban o lo pierde) y cae en malas manos, no es posible desactivarlo, por lo que está expuesto a amenazas como la violación de datos, el secuestro de cuentas o la denegación de servicio, entre otras.

El análisis también ha tenido en cuenta los **aspectos legales y jurídicos**. Puede destacarse que no existe una legislación internacional para la protección y tratamiento de datos personales, lo que puede perjudicar tanto a los proveedores de servicios, que pueden tener sus centros de datos repartidos entre varios continentes con legislaciones diferentes, como a los propios usuarios, que pueden quebrantar las leyes de su propio país si lo datos se almacenan en países terceros. Desde el punto de vista de un usuario español, tanto la legislación española como la de la Unión Europea son muy restrictivas, con el objetivo de asegurar la máxima protección para los datos de sus ciudadanos, y cualquier movimiento de datos personales fuera de la UE debe ser justificado y aprobado por la AEPD (en caso de proveedores y usuarios españoles). Por tanto, a día de hoy, trabajar con un servicio de almacenamiento de datos ubicado en la UE parece más seguro, con el fin de garantizar la protección de datos personales, al menos legalmente, que trabajar con proveedores de, por ejemplo, Rusia o Estados Unidos.

7. Conclusiones

Uno de los principales servicios ofrecidos en la nube es el almacenamiento de datos. Este servicio, que puede clasificarse en público, privado o híbrido, permite a sus proveedores proporcionar almacenamiento bajo demanda y almacenar ingentes cantidades de datos de sus usuarios. Ofrece ventajas tales como la reducción del coste de almacenamiento inherente a los dispositivos tradicionales o el acceso a los datos desde cualquier dispositivo y lugar con conexión a Internet.

Debido a toda la información que transmiten y almacenan los diferentes proveedores y usuarios, el almacenamiento en la nube es un objetivo muy atractivo para los atacantes. Se enfrenta a multitud de amenazas que ponen en riesgo la seguridad de los datos de sus usuarios o la credibilidad del propio proveedor del servicio; siendo una de las principales barreras para la adopción del almacenamiento en la nube. Muchas de estas amenazas han sido presentadas y descritas por entidades especializadas en la seguridad en la nube, junto con propuestas para mitigar su impacto en caso de materializarse. Paralelamente, han ido apareciendo trabajos en los que se definen los principales requisitos de seguridad que deberían cumplir los productos que dan acceso al servicio de almacenamiento en la nube público y que tienen como fin mitigar el impacto de determinados ataques.

Hoy en día, existen muchos productos que dan acceso al servicio de almacenamiento en la nube, servicio ofrecido pública y, en parte, gratuitamente por diferentes proveedores. Al seleccionar el producto de un proveedor determinado, los usuarios deberían poder decidir si se adapta a sus requisitos de seguridad antes de escogerlo definitivamente. Es decir, deberían poder realizar un **análisis de seguridad** o consultar los realizados por terceros, sobre todo cuando los usuarios sean organizaciones; es complicado que los usuarios particulares sean capaces de realizar un análisis de seguridad. Con el fin de analizar su seguridad y servir de ejemplo para trabajos futuros, se han seleccionado tres productos de tres proveedores distintos, pertenecientes a ámbitos geográficos y jurídicos diferentes: Yandex.Disk, CloudMe y Google Drive.

El resultado principal del análisis llevado a cabo es que los tres productos tienen carencias en cuanto a la implementación de los requisitos de seguridad, lo que los hace vulnerables ante algunas de las principales amenazas, siendo la violación de datos la más importante a la que se enfrentan. En general, ninguno de los tres productos parece que haya sido diseñado teniendo en cuenta requisitos de seguridad de datos, a pesar de que se hayan construido algunas capas de seguridad sobre dichos productos. En su documentación se reitera que "*usan la última tecnología para mantener seguros tus archivos*", e incluso, uno de los proveedores (Google Drive) presenta certificaciones de seguridad como la ISO/IEC 27001:2013.

Los usuarios de los servicios de almacenamiento en la nube no deberían estar tranquilos en ningún momento de como guardan y aseguran sus datos los diferentes proveedores. Una elección errónea del proveedor o producto, puede derivar en la violación de su privacidad, pérdida de datos, sanciones económicas si no se cumple la legislación vigente, etc. Finalmente, y dado que el estado del arte demuestra que la seguridad empieza por el propio usuario, se recomienda que futuras investigaciones se centren en proporcionar herramientas que permitan a los usuarios analizar y seleccionar los productos que se adaptan a sus necesidades.

- Página dejada en blanco intencionadamente -

Anexos

Anexo A. Deduplicación de datos

La técnica de **deduplicación de datos** es usada por los proveedores para poder ahorrar espacio de almacenamiento, eliminando redundancias cuando se reciben dos o más copias de los mismos datos. Existen diferentes alternativas de deduplicación [17] [18]:

- Deduplicación en cliente o deduplicación en el servidor.
- Deduplicación *single-user* o deduplicación *cross-user*.
- Deduplicación a nivel de archivo o deduplicación a nivel de bloque.

Deduplicación en cliente o deduplicación en el servidor

La deduplicación puede realizarse en el cliente o en el lado del servidor. En el caso de la **deduplicación en el lado servidor**, el cliente envía los datos al servidor y es éste el encargado de ejecutar los procesos de deduplicación. En el caso de la **deduplicación en el lado cliente**, normalmente, el cliente calcula una función *hash* sobre el archivo a subir, enviando el resultado al servidor, que al recibirlo comprueba si ya tiene una copia del archivo, de modo que sólo se envía si el servidor no posee ninguna copia [17] [18]. Tal y como se vio en el apartado 6.5.1, Yandex.Disk es un ejemplo de deduplicación en el lado cliente.

Si la deduplicación se realiza en el **lado del servidor**, se incurre en un mayor coste de las comunicaciones, puesto que el archivo siempre se envía. Además, si el archivo no ha sido cifrado previamente por el usuario (utilizando su clave) antes de subirlo, se corre el riesgo de que se pueda **violar su confidencialidad**. En cambio, si se realiza en el **lado del cliente**, el usuario puede obtener información que le indique si el archivo ya existía en el sistema de almacenamiento o no. En el caso de que además se utilice la deduplicación *cross-user*, un atacante podría aprovecharlo para **extraer información** la siguiente información [17]:

- Conocer qué archivos están almacenados en un proveedor, observando la cantidad de bytes transmitidos al subir un archivo.
- Obtener información de un usuario específico del servicio. El atacante podría subir diferentes versiones de un mismo documento, presumiblemente relacionado con la víctima, y deducir, dependiendo de los bytes transmitidos, qué versión es la correcta, consiguiendo por tanto violar su privacidad.

Deduplicación *single-user* o deduplicación *cross-user*

Con la **deduplicación *single-user***, sólo se comprueba la existencia de los archivos en la cuenta del usuario que sube el archivo. En cambio, usando la **deduplicación *cross-user***, la comprobación se realiza entre todos los usuarios del servicio de almacenamiento [18].

La deduplicación ***single-user*** permite preservar de forma más eficaz la confidencialidad de los archivos transmitidos, puesto que no debe realizar las comprobaciones entre los distintos usuarios del servicio. La deduplicación ***cross-user*** presenta problemas para la seguridad de los datos si se combina con la deduplicación en el lado del cliente, aunque es más eficiente en cuanto a costes, ya que permite un mayor ahorro del espacio requerido [18]. Yandex.Disk es un ejemplo de deduplicación *cross-user*.

Deduplicación a nivel de archivo o deduplicación a nivel de bloque

Indica a qué nivel de profundidad se lleva a cabo la deduplicación. Si se realiza a **nivel de archivo**, ésta simplemente se deduplica a nivel de fichero. En cambio, a **nivel de bloques**, los archivos se dividen en bloques y se realiza el proceso de deduplicación a nivel de cada bloque que compone el archivo [18].

En el caso de que se use deduplicación a **nivel de archivo y *cross-user***, puede deducirse que algún otro usuario tiene exactamente el mismo archivo (si los archivos no están cifrados). Si se hace a **nivel de bloque**, un atacante puede realizar un ataque que combine fuerza bruta con la elección de archivos, manipulados adecuadamente, para obtener partes específicas de un archivo [18].

Anexo B. Suites de cifrado aparecidas durante el estudio

En este anexo, se describen algunas de las características principales de las **suites de cifrado** para el protocolo seguro de comunicaciones TLS y que han ido apareciendo durante el análisis de los productos de almacenamiento en la nube estudiados.

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (Yandex.Disk)

- Algoritmo de intercambio de claves: ECDHE_RSA. La clave simétrica se genera con el algoritmo *Ephemeral Elliptic curve Diffie–Hellman* (ECDHE), que se firma con el algoritmo RSA para su autenticación [39]. Proporciona *Perfect Forward Secrecy* [51].
- Cifrado de mensajes: uso del algoritmo AES con clave de 128 bits, establecida entre el cliente y el servidor, en modo *Galois/Counter*. Proporciona confidencialidad y autenticación del origen de datos [52].
- Verificación de integridad de los mensajes: cálculo del MAC (*Message Authentication Code*) con la función *hash* SHA-256 [53].

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (CloudMe)

- Algoritmo de intercambio de claves: ECDHE_RSA.
- Cifrado de mensajes: uso del algoritmo AES con clave de 256 bits en modo *Galois/Counter*. Proporciona confidencialidad y autenticación del origen de datos [52].
- Verificación de integridad de los mensajes: cálculo del MAC con la función *hash* SHA-384 [53].

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (Google Drive TLS 1.1)

- Algoritmo de intercambio de claves: ECDHE_ ECDSA. La clave simétrica se genera con el algoritmo ECDHE, que se firma con el *Elliptic Curve Digital Signature Algorithm* (ECDSA) para su autenticación [39]. Proporciona *Perfect Forward Secrecy* [51].
- Cifrado de mensajes: uso del algoritmo AES con clave de 128 bits en modo *Cipher Block Chaining*.
- Verificación de integridad de los mensajes: cálculo del MAC con la función *hash* SHA-1 [53].

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (Google Drive TLS 1.2)

- Algoritmo de intercambio de claves: ECDHE_ ECDSA.
- Cifrado de mensajes: uso del algoritmo AES con clave de 128 bits en modo *Galois/Counter*. Verificación de integridad de los mensajes: cálculo del MAC con la función *hash* SHA-256 [53].

Anexo C. Aplicaciones de cifrado en el cliente

A continuación, se hace una relación de algunos productos y sus características para el cifrado de archivos y carpetas en el lado cliente de los servicios de almacenamiento. Permiten, por tanto, trasmitir los datos y almacenarlos en las instalaciones del proveedor completamente cifrados. Es aconsejable que los usuarios usen estos tipos de aplicaciones antes de subir sus archivos a la nube.

Aplicación	Plataformas	Compatibles con Proveedores	Características
BoxCryptor	Microsoft Windows Mac OS X iOS Android Microsoft Windows Phone Microsoft Windows RT Blackberry 10 Google Chrome (Plug-in)	Google Drive Dropbox Box OneDrive Amazon S3 Amazon Cloud Drive iCloud Drive Yandex.Disk CloudMe ownCloud SpiderOak otros	• Cifrado AES-256 y RSA. • Cifrado de archivos al vuelo. • Todo el cifrado y descifrado se realiza en el lado cliente. • Acceso seguro para compartir archivos. • Cifrado de nombre de archivo. • Optimizado para trabajo en equipo • Llave maestra. • Restablecimiento de contraseña. • Definición de políticas.
nCrypted Cloud	Microsoft Windows Mac OS X iOS Android	Google Drive Dropbox OneDrive Box Egnyte	• Guarda la información en un contenedor Zip en el lado cliente. • Cifrado AES-256 para proteger el Zip. • Uso de una única contraseña por archivo. • Todo el cifrado y descifrado se realiza en el lado cliente.
Viivo	Microsoft Windows Mac OS X iOS Android	Dropbox Box Google Drive OneDrive	• Cada usuario tiene una clave privada, cifrada con AES-256, y que se genera a partir de la contraseña del usuario. • Cifrado de archivos con AES-256. Para cada archivo se genera una única clave de cifrado. • Permite compartir de directorios, para los que se crea una clave de compartición.
Sookasa	Microsoft Windows Mac OS X iOS Android	Dropbox Box Google Drive OneDrive Slack Salesforce Zendesk	• Cifrado de archivos con AES-256. • Cifrado automático en los dispositivos. • Separación de la clave de cifrado y los datos cifrados. • Gestiona la distribución de las claves de cifrado.

Aplicación	Plataformas	Compatibles con Proveedores	Características
			• Controla el acceso a los recursos almacenados. • Mantiene una auditoria de acceso a los archivos cifrados.
Cloudfogger	Microsoft Windows Mac OS X (beta) iOS Android	Dropbox Google Drive OneDrive Box SugarSync Mega VirtualDrive Strato HiDrive GoodSync OwnCloud Bitcasa 1&1 SmartDrive Telekom Mediencenter	• Cifrado de archivos con AES-256. • Clave AES única por archivo, almacenada con el mismo archivo. • Cifrado automático en los dispositivos.

Anexo D. Sistemas de almacenamiento

En este apartado se introducirán algunos los sistemas de almacenamiento más usados hoy en día. Dependiendo de las características que se quieran proveer, es de gran importancia seleccionar el sistema adecuado, ya que éste impactará en el éxito o fracaso del servicio almacenamiento en la nube que se quiera prestar. Existen diferentes sistemas de almacenamiento hoy en día, cada uno con sus ventajas y limitaciones, algunos de los cuales se introducen a continuación [8] [19].

Sistemas de almacenamiento de objetos. Proporcionan la infraestructura necesaria para poder almacenar y extraer los datos en forma de objetos de tamaño flexible y sin limitaciones, en cuanto al número de objetos individuales que pueden crearse; por ejemplo, *Amazon S3* y *Google* Almacenamiento en la nube indican que los objetos puedes contener hasta 5 TB de datos. Su arquitectura está diseñada para que todos los nodos de almacenamiento distribuidos se vean como un único *pool*, permitiendo de esta forma su escalabilidad masiva e ilimitada, así como una gestión más sencilla. Manteniendo múltiples copias de los datos entre los diferentes nodos se mejora la disponibilidad y la durabilidad de la información. Son útiles cuando múltiples servidores intentan acceder simultáneamente a los datos almacenados y es necesario un acceso *nearonline* al almacenamiento.

Sistemas de almacenamiento de bloques. Permiten el acceso a dispositivos basados en bloques, el cual es el almacenamiento de nivel más bajo y fundamental para la construcción del resto de sistemas de almacenamiento. Son sistemas apropiados para aplicaciones que necesitan acceso rápido y de bajo nivel a disco. Funcionan muy bien con bases de datos y otras aplicaciones diseñadas para trabajar con los sistemas de archivos de *Linux* o *Microsoft Windows*. [8] [19].

Sistemas *Distributed File Storage*. El almacenamiento de archivos es la tecnología usada, entre otros, en los discos duros y sistemas *NAS*, permitiendo el acceso a la información mediante el nombre y la ruta del archivo. Ofrece sistemas de bajo coste, pero con una latencia bastante alta, siendo apropiados para sistemas en los que la información debe retenerse durante bastante tiempo, aunque deje de usarse. [8] [19].

Siglas y acrónimos

AEPD: Agencia Española de Protección de Datos.

AES: *Advanced Encryption Standard.*

API: *Application Programming Interface.*

BDD: Base de datos.

CDMI: *Cloud Data Management Interface.*

CIA: *Central Intelligence Agency* de EE.UU.

CRM: *Customer relationship management*.

CSA: *Cloud Security Alliance*.

ECDHE: *Ephemeral Elliptic curve Diffie–Hellman*.

ECDSA: *Elliptic Curve Digital Signature Algorithm*.

EMA: *Enterprise Management Associates*.

ENISA: Agencia Europea de Seguridad de las Redes y de la Información.

IaaS: *Infrastructure as a Service*.

INCIBE: Instituto Nacional de Ciberseguridad de España.

LOPD: Ley Orgánica de Protección de Datos.

MAC: *Message Authentication Code*.

MD5: *Message-Digest Algorithm 5*.

NIST: *National Institute of Standards and Technology.*

NSA: *National Security Agency* de EE.UU.

OWASP: *Open Web Application Security Project*.

PaaS: *Platform as a Service*.

RSA: Sistema criptográfico de clave pública descrito por Rivest, Shamir y Adleman.

SaaS: *Software as a Service*.

SHA: *Secure Hash Algorithm*.

SIT: *Fraunhofer Institute for Secure Information Technology*.

SNIA: *Storage Networking Industry Association*.

SSL: *Secure Sockets Layer*.

TLS: *Transport Layer Security*.

Índice de figuras

Índice de tablas

Bibliografía

[1]: Observatorio de la Seguridad de la Información del Instituto Nacional de Tecnologías de la Comunicación (INTECO). Guía para empresas: Seguridad y Privacidad del *Cloud Computing*. Ministerio de Industria, Turismo y Comercio. Gobierno de España. Octubre 2011. URL: http://www.inteco.es (último acceso en Noviembre 2015).

[2]: Bhavani Thuraisingham. Devoloping and Securing the Cloud. CRC Press. © 2014 by Taylor & Francis Group, LLC.

[3]: Esquema Nacional de Seguridad (ENS). Guía de Seguridad de las TIC (CCN-STIC-823). Utilización de Servicios en la Nube. Ministerio de la Presidencia. Gobierno de España. Diciembre 2014. © Editor y Centro Criptológico Nacional, 2014.

[4]: Peter Mell and Timothy Grance. The NIST Definition of Cloud Computing. Special Publication 800-145. Recommendations of the National Institute of Standards and Technology. September 2011.

[5]: Vic (J.R.) Winkler. Securing the Cloud. Cloud Computer Security Techniques and Tactics. © 2011 Elsevier Inc. All rights reserved.

[6]: Raghu Yeluri and Enrique Castro-León. Building the Infraestructures for Cloud Security. Apress Open. © 2014 by Apress Media, LLC, all rights reserved. AppressOpen Rights.

[7]: Cloud Security Alliance (CSA). Security Guidance for Critical Areas of focus in Cloud Computing V3.0. © 2011. All rights reserved. November 2011. URL: https://cloudsecurityalliance.org/ (último acceso en Noviembre 2015).

[8]: Greg Schulz. Cloud and Virtual Data Storage Networking. CRC Press. © 2012 by Taylor & Francis Group, LLC.

[9]: Tom Leyden. A Beginner's Guide to Next Generation Object Storage. © 2013 DataDirect Networks. All rights reserved. URL: http://www.ddn.com (último acceso en Octubre 2015).

[10]: Amazon AWS. URL: https://aws.amazon.com (último acceso en Diciembre 2015).

[11]: *Website* de TechTarget. URL: http://www.techtarget.com/ (último acceso en Diciembre 2015).

[12]: *Website* de Webopedia. URL: http://www.*web*opedia.com/ (último acceso en Octubre 2015).

[14]: Instituto Nacional de Tecnologías de la Comunicación (INTECO). Riesgos y Amenazas en Cloud Computing. INTECO-CERT. Ministerio de Industria, Turismo y Comercio. Gobierno de España. Marzo 2011. URL: http://www.inteco.es (último acceso en Diciembre 2015).

[15]: SNIA. Cloud Data Management Interface. Version 1.1.1. Copyright © 2015 SNIA. All rights reserved. URL: http://www.snia.org/ (último acceso en Noviembre 2015).

[16]: Aaron Wheeler and Michael Winburn. Cloud Storage Security. A practical guide. Copyright © 2015 Elsevier Inc. All rights reserved

[17]: Moritz Borgmann, Tobias Hahn, Michael Herfert, Thomas Kunz, Marcel Richter, Ursula Viebeg and Sven Vowé. On the Security of Cloud Storage Services. SIT Technical Reports SIT-TR-2012-001. © by FRAUNHOFER VERLAG, 2012.

[18]: Jesús Díaz Vico. Seguridad en servicios de almacenamiento. Análisis de Dropbox y Mega. Instituto Nacional de Ciberseguridad (INCIBE). Diciembre 2014. URL: https://www.incibe.es (último acceso en Diciembre 2015).

[19]: In Cloud Planning, Make Room for Storage. Handbook. TechTarget. URL: http://searchcloudcomputing.techtarget.com (último acceso en Noviembre 2015).

[20]: Data Breach IM ACYF-CB-IM-15-04 (F). U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES Administration for Children and Families. July 2015. URL: http://www.acf.hhs.gov/ (último acceso en Noviembre 2015).

[21]: ISO/IEC 27040:2015. Information technology -- Security techniques -- Storage security. URL: https://www.iso.org (último acceso en Noviembre 2015).

[22]: Cloud Security Alliance. The Notorious Nine. Cloud Computing Top Threats in 2013. Top Threats Working Group. February 2013. © 2013 Cloud Security Alliance – All Rights Reserved.

[23]: MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. © Ministerio de Hacienda y Administraciones Públicas. Secretaría General Técnica. Subdirección General de Información, Documentación y Publicaciones Centro de Publicaciones. Octubre 2012. URL: http://administracionelectronica.gob.es/ (último acceso en Noviembre 2015).

[24]: Agencia Europea de Seguridad de las Redes y de la Información (ENISA). Computación en nube. Beneficios, riesgos y recomendaciones para la seguridad de la información. Edición en castellano. Noviembre 2009. URL: http://www.enisa.europa.eu/ (último acceso en Octubre 2015).

[25]: Agencia Europea de Seguridad de las Redes y de la Información (ENISA). Cloud Security Guide for SMEs. Cloud computing security risks and opportunities for SMEs. Edición en inglés. Abril 2015. URL: http://www.enisa.europa.eu/ (último acceso en Diciembre 2015).

[26]: Danan Thilakanathan, Shiping Chen, Surya Nepal and Rafael A. Calvo. Secure Data Sharing in the Cloud. S. Nepal and M. Pathan (eds.), Security, Privacy and Trust in Cloud Systems, DOI: 10.1007/978-3-642-38586-5_2, © Springer-Verlag Berlin Heidelberg 2014.

[27]: Safe Harbor Framework. URL: http://www.export.gov/safeharbor/index.asp (último acceso en Diciembre 2015).

[28]: Un estudio de Symantec indica que los empleados roban datos corporativos y piensan que estas acciones son aceptables. URL: https://www.symantec.com/ (último acceso en Diciembre 2015).

[29]: ENTERPRISE MANAGEMENT ASSOCIATES. State of File Collaboration Security. File Insecurity: The Final Data Leakage Frontier. An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper Prepared for FinalCode, Inc. September 2015.

[30]: CNN Money. Google loses data after lightning strikes. August 2015 URL: http://money.cnn.com/ (último acceso en Diciembre 2015).

[31]: Google Compute Engine Incident #15056. Google Compute Engine Persistent Disk issue in europe-west1-b. August 2015. URL: https://status.cloud.google.com/ (último acceso en Noviembre 2015).

[32]: ComputerWeekly.com. Ashley Madison data breach escalates with password encryption failure. URL: http://www.computerweekly.com/news/ (último acceso en Noviembre 2015).

[33]: Mathew J. Schwartz. New Virtualization Vulnerability Allows Escape To Hypervisor Attacks. Dark Reading. InformationWeek. Mathew J. Schwartz. June 2012. URL: http://www.darkreading.com/ (último acceso en Noviembre 2015).

[34]: Paul Ducklin. Dropbox lets anyone log in as anyone - so check your files now! NakedSecurity. Sophos. June 2011. URL: https://nakedsecurity.sophos.com/ (último acceso en Noviembre 2015).

[35]: Adam Greenberg. Northwestern Memorial HealthCare laptop stolen, patient data at risk. SC Magazine. December 2012. URL: http://www.scmagazine.com/ (último acceso en Noviembre 2015).

[36]: Joshua Davies. Implementing SSL/TLS Using Cryptography and PKI. Copyright © 2011 by Wiley Publishing, Inc., Indianapolis, Indiana.

[37]: OWASP. Testing for User Enumeration and Guessable User Account (OWASP-AT-002). URL: https://www.owasp.org/index.php/Testing_for_User_Enumeration_and_Guessable_User_Account (último acceso en Diciembre 2015).

[38]: Yadex Support Disk. URL: https://yandex.com/support/disk/ (último acceso en Diciembre 2015).

[39]: IETF. RFC5289 - TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM). URL: https://tools.ietf.org/html/rfc5289 (último acceso en Diciembre 2015).

[40]: Certum by Unizeto. URL: http://www.certum.eu/certum/cert,eindex_en.xml (último acceso en Noviembre 2015).

[41]: Wikipedia. EICAR Standard Anti-Virus Test File. URL: https://es.wikipedia.org/wiki/EICAR (último acceso en Noviembre 2015).

[42]: Agencia Española de Protección de Datos – AEPD. URL: https://www.agpd.es (último acceso en Diciembre 2015).

[43]: Yandex Legal Documents. URL: https://yandex.com/legal/ (último acceso en Noviembre 2015).

[44]: Yandex. RT. Junio 2015. URL: https://actualidad.rt.com/ (último acceso en Noviembre 2015).

[45]: Reuters. Russia's Yandex to open new office in Europe. URL: http://in.reuters.com/ (último acceso en Noviembre 2015).

[46]: CloudMe. URL: https://www.cloudme.com (último acceso en Diciembre 2015).

[47]: Foro oficial de CloudMe. URL: http://forum.cloudme.com/index.php (último acceso en Diciembre 2015).

[48]: OWASP. Authentication Cheat Sheet. URL: https://www.owasp.org/index.php/Authentication_Cheat_Sheet (último acceso en Noviembre 2015).

[49]: Elisenda Bru Cuadrada. La protección de datos en España y en la Unión Europea. Especial referencia a los mecanismos jurídicos de reacción frente a la vulneración del derecho a la intimidad. Monográfico «III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas». IDP. REVISTA DE INTERNET, DERECHO Y POLÍTICA. Septiempre de 2007. URL: http://idp.uoc.edu (último acceso en Diciembre 2015).

[50]: Página principal de Google. URL: https://www.google.com (último acceso en Diciembre 2015).

[51]: IETF. RFC4492 - Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS). URL: https://tools.ietf.org/html/rfc4492 (último acceso en Diciembre 2015).

[52]: IETF. RFC5288 - AES Galois Counter Mode (GCM) Cipher Suites for TLS. URL: https://tools.ietf.org/html/rfc5288 (último acceso en Diciembre 2015).

[53]: IETF. RFC5246 - The Transport Layer Security (TLS) Protocol Version 1.2. URL: https://www.ietf.org/rfc/rfc5246.txt (último acceso en Diciembre 2015).

[54]: Google Identity Platform. URL: https://developers.google.com/identity/choose-auth (último acceso en Diciembre 2015).

[55]: Google Centros de datos. URL: https://www.google.com/about/datacenters/inside/locations/index.html (último acceso en Diciembre 2015).

[56]: SoapUI. © 2015 SmartBear Software. All rights reserved. URL: http://www.soapui.org/ (último acceso en Diciembre 2015).

[57]: Página de soporte de Google. URL: https://support.google.com (último acceso en Diciembre 2015).

[58]: Skyhigh. Cloud Adoption and Risk Report – Q4 2014. Published Q1 2015. URL: http://www.isaca.org/chapters1/Northeast-Ohio/events/Documents/Skyhigh Cloud Adoption and Risk Report - Q4 2014.pdf (último acceso en Diciembre 2015).

[59]: Web Empires. World map of dominating websites. URL: http://webempires.org/blog/dominating-websites-map/ (último acceso en Diciembre 2015).

[60]: Dr. Web. Wikipedia. URL: https://en.wikipedia.org/wiki/Dr._Web (último acceso en Diciembre 2015).

[61]: Wikipedia. Edward Snowden. URL: https://en.wikipedia.org/wiki/Edward_Snowden (último acceso en Diciembre 2015).

[62]: Dispositivos utilizados recientemente en Google. URL: https://security.google.com/settings/security/activity (último acceso en Diciembre 2015).