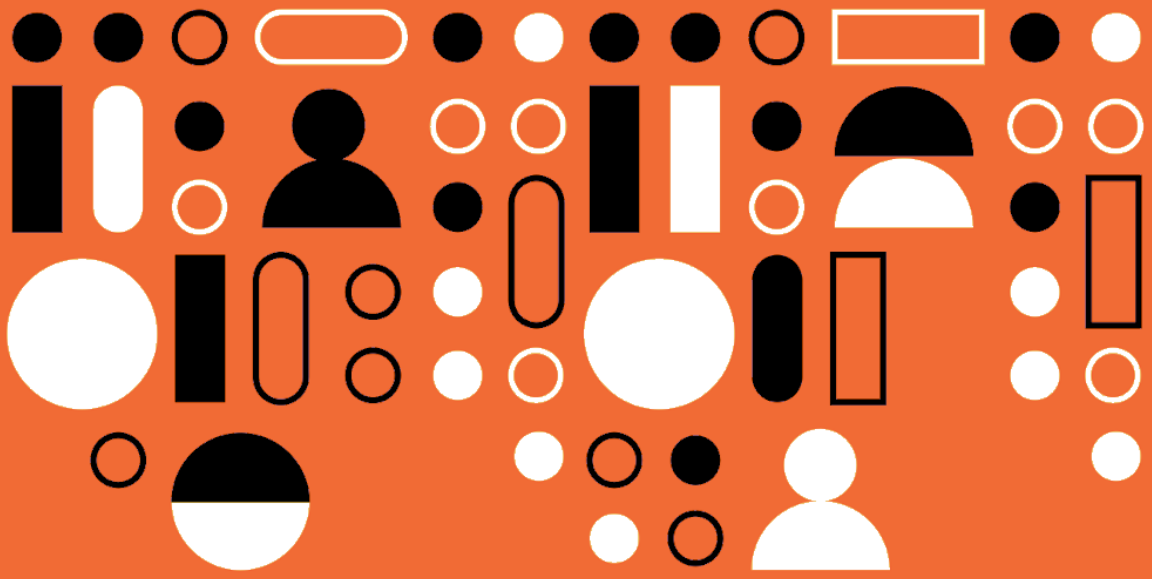
CONTRATACIÓN DE SERVICIOS EDUCATIVOS EN LA NUBE



Riesgos y recomendaciones desde la perspectiva de la protección de datos personales

Contratación de servicios educativos en la nube.

Riesgos y recomendaciones desde la perspectiva de la protección de datos personales

Patricia Díaz Charquero y Mariana Fossatti [1]

Palabras clave: Protección de datos personales, Instituciones Educativas, Contratación de servicios educativos cloud

Actualmente se observa una enorme irrupción de servicios de tecnología educativa basados en el cloud computing, así como la creciente interoperabilidad de estos servicios. De estas tecnologías surgen muchas posibilidades de innovación en el ámbito educativo, pero también diversas incertidumbres y desafíos. El almacenamiento y la posibilidad de tratamiento masivo de datos de estudiantes permite acumular información y generar perfiles personales desde la temprana edad en que comienzan la actividad escolar y durante todo su tránsito educativo. En este nuevo contexto surge la disyuntiva entre confiar ciegamente en las soluciones tecnológicas o analizarlas con una mirada crítica que permita evaluar sus implicancias legales y éticas. En este artículo brindamos elementos para que las IEs puedan responder, al menos, estas preguntas: ¿qué es la computación en la nube?, ¿qué aspectos evaluar al momento de optar por las diferentes soluciones de tecnología educativa disponibles?, ¿cuáles son los principales riesgos en materia de privacidad y protección de datos personales al momento de contratar servicios de educativos en la nube?

1- ¿Qué es la computación en la nube?

Si bien no existe una definición universalmente aceptada de computación en la nube o

1 Patricia Díaz-Charquero investigadora en DATYSOC, Montevideo, Uruguay (e-mail: pdiaz@oce.edu.uy). Mariana Fossatti investigadora en DATYSOC, Montevideo, Uruguay (e-mail: mfossatti@gmail.com) DATYSOC: Grupo de investigación que busca proporcionar una evaluación del estado actual del arte de la vigilancia de las comunicaciones, de la privacidad y de la ciberseguridad en Uruguay (http://datysoc.org/).

“Cloud Computing”, existen organismos internacionales cuyos objetivos son la estandarización de Tecnologías de la Información, y específicamente de las tecnologías basadas en la nube. El Information Technology Laboratory del NIST (Agencia del departamento de comercio de los Estados Unidos) se encarga de los estándares de las tecnologías de la información y define al Cloud Computing como:

> “Un modelo que permite el acceso bajo demanda a través de la Red a un conjunto compartido de recursos de computación configurables (por ejemplo: redes, servidores, almacenamiento, aplicaciones y servicios) que se pueden aprovisionar rápidamente con el mínimo esfuerzo de gestión o interacción del proveedor del servicio” (Traducción nuestra) (Mell, Grance, & others, 2011)

Este modelo implica la posibilidad de que los diferentes recursos físicos (como por ejemplo almacenamiento, procesamiento, memoria, ancho de banda de la red y máquinas virtuales) sean asignados y reasignados dinámicamente, de modo que el cliente, normalmente, no tiene control ni conocimiento sobre la posición exacta de los recursos proporcionados.

2 - Modelos de computación en la nube según tipo de acceso

De las diferentes clasificaciones de modelos de computación en la nube realizadas por el NIST, nos interesa particularmente describir la clasificación relacionada con el *tipo de acceso*, ya que este condiciona la posibilidad de control efectivo de los datos.

De acuerdo a esta clasificación, encontramos que los centros de datos virtualizados pueden utilizar modelos de nube privada, nube pública o nube híbrida.

La «**nube privada**» es una infraestructura informática (máquinas, redes, almacenamiento, centros de datos, etc) dedicada a una organización individual; está situada en las instalaciones de la propia organización o bien su gestión está subcontratada a un tercero (normalmente a través de alojamiento de servidores). Una de las características que hace atractiva este tipo de nube para una organización,

es el grado de control y de privacidad de los datos, ya que los recursos se encuentran bajo el estricto control de la propia organización (no nos referimos al grado de seguridad pues la seguridad depende de varios factores).

Una «**nube pública**», por el contrario, es una infraestructura propiedad de un proveedor especializado en la prestación de servicios de nube que pone a disposición (y, por consiguiente, comparte) sus sistemas con los usuarios u organizaciones que contratan sus servicios. Se accede al servicio a través de Internet, lo que implica la transferencia de actividades de tratamiento de datos a los sistemas del proveedor de servicios. Desde el punto de vista de la protección de datos personales, la consecuencia más destacable del uso de este tipo de nube es que el responsable del tratamiento está obligado a transferir una parte importante del control que ejerce sobre dichos datos y el proveedor de servicios desempeña un papel clave en lo que refiere a la protección eficaz de los datos personales almacenados en sus sistemas.

Por último, además de las nubes «públicas» y «privadas» encontramos **«nubes híbridas»**, donde el usuario es propietario de parte de la infraestructura y combina esta modalidad con servicios adquiridos en nubes públicas.

Como mencionamos anteriormente entendemos que las soluciones tecnológicas no son neutras y, si analizamos la estructura de cada modelo, encontramos una tensión importante entre las **soluciones orientadas a optimizar costes (perdiendo el control sobre la infraestructura y los datos) y las soluciones orientadas a garantizar los derechos de los usuarios**. Lamentablemente, para muchas instituciones no es viable o sostenible a largo plazo el uso de una nube privada, principalmente por razón de costes. Consideramos que al Estado, a través de las Unidad Reguladora y de Control de Datos Personales (URCDP, s. f.), le corresponde apoyar a las IEs al momento de tomar este tipo de decisiones y proporcionar elementos para evaluar opciones.

3 - Las grandes corporaciones de la información y los servicios educativos en la nube

El campo de las tecnologías educativas parece estar reclamando en la actualidad la denominación de “industria” por derecho propio. Se habla de un mercado potencialmente gigantesco que no es tan sólo un subsector dentro de la industria del software. Según el informe de EdTechXGlobal, conferencia global de negocios en tecnología educativa, aunque se calcula que solamente el 2% de la educación está digitalizada, el mercado actual estaría creciendo a una tasa de 17% anual y alcanzaría el valor de 252 mil millones de dólares en 2020 (EdTechXGlobal, s. f.). Cifras millonarias similares a estas se repiten en los medios especializados de este sector, con considerables variaciones en su magnitud, pero siempre desde una narrativa que hace énfasis en el potencial de este codiciado mercado educativo.

Dentro de esta industria destacan algunas compañías nacidas como startups educativas, como Udacity, Coursera, Edmodo y otras, valoradas en millones de dólares. El sector también comprende tecnologías y proyectos libres con modelos de negocio abiertos, como Moodle, de amplio uso para la gestión de aulas virtuales. Sin embargo, también están desarrollando sus negocios en esta área grandes corporaciones: Google, Apple, Amazon, Microsoft y Facebook, que desarrollan productos con sus marcas o adquieren y financian *startups*.

Una y otra vez, en informes y análisis de consultoras, se repite que estas corporaciones aprovecharán “sus potentes plataformas”, “su ecosistema”, “su enorme base de usuarios” para imponerse en el ámbito educativo. No siempre se comenta que también se basan en una importante capacidad de *lobby* para ganarse grandes clientes institucionales, tanto de la educación pública como privada (Singer, 2017) [2] Además, en muchas ocasiones las ofertas de productos de tecnologías educativas por parte de las corporaciones viene acompañado de una narrativa filantrópica. Los vínculos comerciales entre ellas y los gobiernos se inician muchas veces como acciones de cooperación para mejorar la educación y brindar acceso universal a herramientas e incluso conectividad a poblaciones con carencias. Como antecedentes podemos nombrar la estrategia de la Compañía Google que provee la suite Google Apps for Education de forma gratuita al sistema educativo público de varios países en desarrollo («Islands in the cloud», s. f.), (Magdirila, Phoebe, 2013), (Koetsier, John, s. f.), («Acuerdo Ceibal-ANEP-Google», 2015).

La preocupación por la privacidad y la protección de datos en educación ha surgido como debate público a partir de la irrupción de estas grandes corporaciones en

2En un informe de la periodista de tecnologías Natasha Singer, publicado en el *New York Times* el 13 de mayo de 2017, se explican detalladamente estas prácticas de lobby a distintos niveles, desde los docentes, hasta las autoridades educativas locales y estatales en EEUU.

educación. Estas preocupaciones, expresadas por distinto tipo de actores, se ven reflejadas en informes gubernamentales, como el realizado por la Agencia Española de Protección de Datos Personales, o en análisis críticos desarrollados por organizaciones no gubernamentales, como las preguntas frecuentes acerca de servicios educativos en la nube y dispositivos en las escuelas de la EFF (Electronic Frontier Foundation, 2015), o las campañas activistas de la Parent Coalition for Student Privacy, (2017) en Estados Unidos. En Uruguay este debate surgió por primera vez en la opinión pública a raíz de un acuerdo entre el Plan Ceibal y Google por el cual el primero accedía gratuitamente a los servicios de Google Apps For Education («Sobre el acuerdo Google-ANEP-Ceibal y sus diferentes dimensiones», 2015).

Estos debates ponen de relieve que, aunque los servicios educativos en la nube tienen grandes ventajas, también son notables sus riesgos desde la perspectiva de la protección de datos, exponiendo a los estudiantes a niveles de vigilancia difíciles de percibir y controlar.

4 - Principales riesgos relacionados con la contratación de servicios en la nube

Las tecnologías educativas que se utilizan en las escuelas y universidades comprenden un amplio espectro de herramientas: desde dispositivos hasta aplicaciones, pasando por servicios de nube o *cloud*. Estos servicios cloud pueden consistir en campus y aulas virtuales, de carácter específicamente educativo, así como en servicios de redes sociales, webmail y almacenamiento en la nube. Las grandes corporaciones de internet, como expusimos previamente, están fuertemente implicadas en este mercado, a través de servicios *cloud* como Google Apps For Education, o Microsoft in Education.

Como vimos, hay diversos modelos de implementación de estos servicios, que pueden ser provistos por la IE o subcontratados. Si bien en ambos casos, los servicios tienen que respetar la legislación vigente en materia de protección de datos, la subcontratación a terceros implica riesgos que hay que tener en cuenta especialmente. El *Grupo de Trabajo sobre Protección de Datos del Artículo 29*[3] (en adelante *GT 29-UE*)

3El Grupo de Trabajo del Artículo 29 (GT 29), creado por la Directiva 95/46/CE, reúne a todos las Autoridades de Protección de Datos de los países de la UE.

detecta **dos riesgos principales** (Grupo de Trabajo del Artículo 29, 2012), que habrá que evaluar de acuerdo al volumen de datos personales que se maneje, los usuarios alcanzados y el tipo de institución contratante de servicios de nube, estos son:

- **Pérdida de control.** Esta puede expresarse de la siguiente manera: a) falta de disponibilidad (dependencia respecto del proveedor); b) falta de integridad (causada por la puesta en común de los recursos en la nube); c) falta de confidencialidad; d) falta de posibilidad de intervención debido a la complejidad y la dinámica de la cadena de subcontratación; e) falta de posibilidad de intervención; f) falta de poder de negociación de las cláusulas contractuales (ya que las ofertas normalizadas son una característica de los servicios de computación en la nube).

- **Falta de información sobre el tratamiento (transparencia).** La ley obliga a que los interesados cuyos datos personales sean objeto de tratamiento en la nube sean informados acerca de la identidad del responsable del tratamiento y de los fines del tratamiento. La principal consecuencia de la falta de transparencia es que la IE que contrata el servicio en la nube, muchas veces no es consciente de las amenazas y riesgos potenciales y por tanto no podrá adoptar las medidas de protección apropiadas. Los datos personales de los usuarios se encuentran en riesgo si la IE, por ejemplo, no conoce:

    - la composición de la cadena de los múltiples encargados del tratamiento y los subcontratistas;

    - si se transmiten datos personales a terceros países que pueden no proporcionar un nivel adecuado de protección de datos;

    - si las transferencias no cuentan con las medidas de protección adecuada.

Pero las IEs, los estudiantes, los padres y los docentes encaran un problema mayor que el del control de proveedores de servicios educativos basados en la nube. Se trata de la **falta de adecuación de los actuales sistemas de protección de datos personales al tratamiento masivo de datos en el ámbito educativo o al “big data en educación”**.

Har Carmel (2016) resume los principales problemas que enfrentan los actuales sistemas de protección de datos:

La re-identificación: el sistema no protege los datos de estudiantes de la re-identificación. Si definimos datos personales como *datos que identifican o hacen identificable a una persona*, basta con anonimizar esos datos para que la ley deje de ser aplicable. El problema aquí, es que resulta bastante cuestionable la anonimización cuando hablamos de *big data* debido a que las técnicas de agregación, derivación contextual y correlación cruzada de grandes volúmenes de información hacen que el riesgo de re-identificación sea muy grande.

La imposibilidad del real consentimiento informado (Opt-in): el principio rector de estos sistemas de protección de datos es el principio del previo consentimiento informado. Aunque excluyamos la posibilidad de ambigüedad en la información proporcionada a los usuarios (o los adultos a cargo en caso de ser menores) por parte de empresas proveedoras de servicios, difícilmente podremos hablar de consentimiento informado frente a la actual capacidad de usos secundarios basados en minería de datos, inclusive cuando se utilizan con fines de mejora en los procesos educativos. Será simplemente demasiado complicado para un estudiante o una madre o padre promedio hacer elecciones conscientes frente al uso inesperado de los datos (Solove, 2013).

La imposibilidad de negarse a dar el consentimiento (Opt-out): por último, Har Carmel plantea la imposibilidad de madres y padres de negarse (opt-out) a brindar su consentimiento, debido a las consecuencias que deberá afrontar si deciden no acompañar la decisión de la IE en cuanto a la selección de proveedores y a la política de privacidad de estos proveedores, ya que no todas las familias tienen la posibilidad de cambiar de IE a sus hijos.

Podemos concluir que, estamos frente a un cambio de paradigma y que, sin lugar a dudas, nos enfrentamos a la necesidad de superar el enfoque de auto-gestión. Solove (2013) y Har Carmel (2016) plantean la re-evaluación del equilibrio de intereses entre sujetos de datos y usuarios de datos mediante un enfoque que considera la privacidad y la protección de datos personales como un nuevo interés colectivo que requeriría una nueva combinación de regulación pública y gestión privada para aumentar el nivel real de protección de la privacidad de los estudiantes.

7 - Recomendaciones para la Contratación de servicios de nube para Educación

Las IEs, como responsables del tratamiento de los datos de estudiantes y docentes, deben cerciorarse de que sus datos personales sean tratados conforme a la Ley 18.331 de Protección de Datos Personales[4] (LPDP, 2008). Esto implica que tienen la responsabilidad de garantizar que su proveedor de servicio en la nube cumple con la LPDP (principio de responsabilidad artículo 12). Será fundamental entonces que presten especial atención a las características de los contratos y a las cláusulas relativas al procesamiento de datos. A continuación planteamos las recomendaciones para la contratación de servicios de nube en Educación:

Necesidad de evaluar Impacto en Privacidad. Antes de contratar las IEs deberían efectuar una evaluación de conveniencia e impacto. Para ello cuentan con el mecanismo de consulta que ofrece la URCDP de AGESIC, siendo recomendable la solicitud de asesoramiento previo a la contratación de servicios en la nube.

Contratos con garantías. Los centros educativos deberán formalizar la contratación de servicios de nube de forma que puedan acreditar su celebración y la incorporación de las garantías adecuadas para la protección de datos personales, incluidas las exigibles en caso de subcontratación. Asimismo, el prestador de servicios de nube debe garantizar la portabilidad de la información y la no conservación de los datos al término del contrato (borrado seguro).

Ubicación de los datos y sub procesadores. Es necesario que los centros educativos conozcan las entidades que intervienen en la prestación de servicios de nube, su ubicación y las garantías adoptadas en caso de que vayan a realizarse transferencias internacionales de datos.

Posibilidad de auditoría. Es preciso que en el contrato se establezca el método o, al menos, la posibilidad de que el centro educativo realice auditorías. El responsable del tratamiento debe mantener el control sobre los datos.

Responsabilidades en materia de seguridad. Es preciso especificar claramente las responsabilidades de todos los intervinientes (IEs, servicios de alojamiento y plataformas educativas) en la implantación de las medidas de seguridad. En particular,

4 Nuestra LPDP considera como dato personal a cualquier tipo de información referida a una persona que la pueda identificar directamente o indirectamente, (como nuestro nombre, dirección, teléfono, cédula de identidad, RUT, huella digital, etc.) y regula de forma particular aquellos datos considerados sensibles (artículo 18)

hay que asegurar la adecuada asignación de permisos de acceso a los datos personales y concienciar a los usuarios sobre los peligros de utilizar contraseñas que no sean suficientemente robustas.

Bibliografía

Ceibal suma herramientas de Google para potenciar el trabajo de docentes y estudiantes - Presidencia de la República. (2015, mayo). [Sala de Medios de Presidencia de la República]. Recuperado 6 de junio de 2017, a partir de https://www.presidencia.gub.uy/comunicacion/comunicacionnoticias/ceibal-suma-herramientas-google-potenciar-trabajo-docentes-estudiantes

EdTechXGlobal. (s. f.). Global Report Predicts EdTech Spend to Reach $252bn by 2020. *PR Newswire*. Recuperado a partir de http://www.prnewswire.com/news-releases/global-report-predicts-edtech-spend-to-reach-252bn-by-2020-580765301.html

Electronic Frontier Foundation. (2015, diciembre 1). FAQ About Cloud Education Services and Devices in Schools. Recuperado 6 de junio de 2017, a partir de https://www.eff.org/issues/student-privacy/faq

Har Carmel, Y. (2016). Regulating'Big Data Education'in Europe: Lessons Learned from the US. *Browser Download This Paper*. Recuperado a partir de https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2772755

Islands in the cloud: Philippines' Department of Education goes Google. (s. f.). Recuperado 6 de junio de 2017, a partir de https://cloud.googleblog.com/2012/09/islands-in-cloud-philippines-department.html

Koetsier, John. (s. f.). Google: 10 million Malaysian students, teachers, and parents will now use Google Apps for Education. *VentureBeat*. Recuperado a partir de https://venturebeat.com/2013/04/10/google-10-million-malaysian-students-teachers-and-parents-will-now-use-google-apps-for-education/

Magdirila, Phoebe. (2013, junio 21). Are Google Apps the New Way to Learn in Philippine

Universities? Recuperado 6 de junio de 2017, a partir de https://www.techinasia.com/google-apps-learn-philippine-universities

Mell, P., Grance, T., & others. (2011). The NIST definition of cloud computing. Recuperado a partir de http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf

Parent Coalition for Student Privacy. (2017, mayo). Parent Toolkit for Student Privacy. Recuperado 6 de junio de 2017, a partir de https://www.studentprivacymatters.org/toolkit/

Parlamento de la República Oriental del Uruguay. Protección de Datos Personales y acción de Habeas Data, Pub. L. No. Ley 18.331 (2008). Recuperado a partir de https://www.impo.com.uy/bases/leyes/18331-2008

Singer, N. (2017, mayo 13). How Google Took Over the Classroom. *The New York Times*. Recuperado a partir de https://www.nytimes.com/2017/05/13/technology/google-education-chromebooks-schools.html

Sobre el acuerdo Google-ANEP-Ceibal y sus diferentes dimensiones. (2015, julio 30). Recuperado 6 de junio de 2017, a partir de https://nogoogleappsedenuy.wordpress.com/2015/07/30/mas-sobre-el-acuerdo-google-anep-ceibal/

Solove, D. (2013). Autogestión de la privacidad y el dilema del consentimiento. *Revista Chilena de Derecho y Tecnología*, *2*(2). https://doi.org/10.5354/0719-2584.2013.30308

URCDP. (s. f.). Unidad Reguladora y de Control de Datos Personales. Recuperado 27 de junio de 2017, a partir de https://www.datospersonales.gub.uy/