Modelo Genérico para la Gestión de Privacidad de Grandes Datos/Big Data

María del Carmen Becerra, María Claudia Gómez, Pedro Zarate

Abstract—**En este trabajo el problema de investigación parte del interrogante de quién son los datos generados y tratados como grandes datos/Big Data. Luego se analiza la hipótesis sobre el conflicto que genera la gestión de la privacidad de los datos personales. Se basa en un modelo donde se identificaron el conjunto de prácticas y recursos de gestión, resultantes de la integración de guías, normas, estándares y obligaciones contractuales más relevantes para mantener a salvo los datos personales y generar confianza en el entorno. En el estudio de campo se muestra la importancia y urgencia de este tema en nuestro país, dado que ello es necesario y presta grandes beneficios para innovar en la gestión empresarial, la prestación de servicios públicos y el diseño e implementación de políticas de desarrollo regional. A través de sus conclusiones se verifica que se necesita una gestión inteligente para rectificar el rumbo en lo que respecta a descubrir y detectar patrones, relaciones y formular modelos a partir de estas gigantescas bases de datos este trabajo presenta un modelo genérico para el manejo de la privacidad en la nube de los enormes volúmenes de datos. Se analiza el impacto de la privacidad, se identifican riesgos y se exploran las soluciones que brindan los estándares para desarrollar controles que se integren en un modelo que permita establecer los pasos para que cualquier tipo de organización pública o privada, pueda verificar el impacto organizacional de sus productos, procesos o servicio, en el cumplimiento de sus objetivos estratégicos.**

Keywords: **Big Data, Estándares, Gestión de bases de datos y grandes datos, Modelos de Datos, Privacidad de Datos, Seguridad.**

I. INTRODUCCION

La gestión y análisis de grandes datos generados por el uso de tecnologías digitales (como la telefonía móvil, las transacciones electrónicas y las redes sociales) son instrumentos eficaces para innovar en la gestión empresarial, la prestación de servicios públicos y el diseño e implementación de políticas de desarrollo. Este fenómeno conocido como Big Data [1] es el conjunto de tecnologías que permiten tratar cantidades masivas de datos provenientes de fuentes dispares, con el objetivo de poder otorgarles una utilidad que les proporcione valor. Es un nuevo paradigma, que alude al enorme crecimiento en el acceso y uso de la información automatizada.

La recolección de datos por las corporaciones y el gobierno amenaza la privacidad mientras promueve la transparencia[1]. Hoy más que nunca, la creciente y enorme cantidad de datos, del orden de zeta bytes, generados por aplicaciones empresariales y de gobierno electrónico ponen en riesgo la privacidad en la nube y determinan la necesidad de un modelo de Integración para la gestión de seguridad de esos enormes conjuntos de datos.

Con el tamaño y complejidad de Big Data llega una infinidad de retos en materia legal y normativa, surgen así una serie de interrogantes: ¿De quién son mis datos?, ¿Por qué las empresas usan mis datos?, ¿De quién son esos enormes volúmenes de datos?, etc., sin embargo la respuesta no es única, la titularidad de los datos presenta muchas aristas según como se los genere y se los trate bajo estrictas medidas de seguridad. Los usuarios regalan sus datos de consumo y localizaciones sobre todo por una vida más cómoda y simple. En el Mobile Congress[2] celebrado el año pasado se muestra en forma inequívoca que están surgiendo nuevos nichos de negocios en áreas como las aplicaciones de salud, mantenimiento preventivo de vehículos, gestión de redes eléctricas, de infraestructuras hídricas y el tratamiento de la información de sensores inteligentes, etc.

Sin embargo todas estas guías, regulaciones, leyes y obligaciones contractuales llegan a ser abrumadoras, por la variedad y multidisciplinariedad que presentan, por lo que se necesitan nuevos modelos de negocios donde la gestión de la privacidad sea técnicamente viable y potencialmente atractiva para el mercado. Ello demandara sin duda algunos modelos futuros donde deberá haber un diálogo ente agentes técnicos, regulatorios, empresariales y civiles.

En este trabajo se analizan estas modulaciones de la subjetividad en la era digital, para establecer pautas comunes que permitan una gestión eficiente y eficaz de los datos generados por los servicios públicos, servicios sociales y servicios financieros, basada en un modelo que permita la integración de estándares más relevantes para mantener a salvo la Privacidad.

28 de Abril de 2017. Instituto de Informática – Laboratorio de Análisis Forense e Informática Jurídica. Departamento de Informática – FCEFN-UNSJ. E- mail: idei@iinfo.unsj.edu.ar, mcbecerra2008@gmail.com, pzarate@iinfo.unsj.edu.ar. Meglioli 1150 (S) Rivadavia- San Juan
Departamento de Informática Facultad de Cs Exactas, Físicas y Naturales UNSJ- Proyecto de Investigación "Representación genérica de modelos conceptuales en el campo de los Sistemas de Información" FCEFN-UNSJ E-mail: cacugomez@yahoo.com.ar

[1] https://mitpress.mit.edu/books/big-data-not-monolith
[2] https://www.mobileworldcongress.com/start-here/2016-highlights/

II. BIG DATA

Tal cual lo expresan Kenneth Neil Cukier and Viktor Mayer Schonberger, los grandes datos empiezan con el hecho que hay mucha información en estos días y hoy más que nunca está disponible para usos extraordinarios. Los grandes datos son más que solo comunicación: La idea es que podemos aprender de un gran cuerpo de información cosas que no podemos comprender cuando usamos solo pequeñas cantidades. Aunque existen varias definiciones de Big Data[3]. A los efectos de este trabajo lo conceptualizaremos [1], como los enormes volúmenes de datos (estructurados, semiestructurados y no-estructurados) del orden de exabytes 10 a 18 bytes), cuyo almacenamiento y análisis[4] (eg) análisis textual de mensajes de correo, Tweets, blogs) se puede hacer mediante base de datos especializadas[5] que sirven para analizar esos enormes volúmenes de datos y conseguir así información y conocimiento[6].

Tal cual lo expresa Gabriel Baum[7] "...es, en el sector de tecnologías de la información y la comunicación, una referencia a los sistemas que manipulan grandes conjuntos de datos (o data sets)". Las dificultades más habituales en estos casos se centran en la captura, el almacenado, búsqueda, compartición, análisis y visualización. La tendencia a manipular ingentes cantidades de datos se debe a la necesidad en muchos casos de incluir los datos relacionados del análisis en un gran conjunto de datos relacionado, tal es el ejemplo de los análisis de negocio, los datos de enfermedades infecciosas, o la lucha contra el crimen organizado.

El límite superior de procesamiento se ha ido desplazando a lo largo de los años, de esta forma los límites que estaban fijados en 2008 rondaban los órdenes de petabytes a zetabytes de datos. En Internet el tráfico durante el año 2016 fue de 1.3 zetabytes según reporte de CISCO[8].

Los científicos con cierta regularidad encuentran limitaciones debido a la gran cantidad de datos en ciertas áreas, tales como la meteorología, la genómica, la conectómica, las complejas simulaciones de procesos físicos, y las investigaciones relacionadas con los procesos biológicos y ambientales, las limitaciones también afectan a los motores de búsqueda en internet, a los sistemas de finanzas y a la informática de negocios.

Los data sets crecen en volumen debido en parte a la introducción de información ubicua procedente de los sensores inalámbricos y los dispositivos móviles (por ej. las VANETs), del constante crecimiento de los históricos de aplicaciones (por ejemplo de los blogs), cámaras (sistemas de teledetección), micrófonos, lectores de radio-frequency identification. La capacidad para almacenar datos de la humanidad se ha doblado a un ritmo de cuarenta meses desde los años ochenta[9].

Las tecnologías relacionadas con el análisis de datos incluyen grandes bases de datos como NOSQL, Hadoop y Map Reduce. La plataforma de código abierto Hadoop se ha convertido en sinónimo de Big Data para buena parte de la industria del almacenamiento y las aplicaciones analíticas. Su adopción aún no es masiva, pero sí progresiva.

Cuando hablamos de Big Data[10], una de las grandes soluciones es sacar todos los datos que están asentados en Data Warehouses y aplicar Data Analytics para entender a dónde quieren llegar los clientes[11]. Por ej. SIRVE (Sistema Integral de Relevamiento Virtual y Estadístico)[12] desarrollado por la Fundación Pescar y Grupo Telecom, brinda a las organizaciones sociales una herramienta de relevamiento de datos, que permite recopilar información con facilidad, eficacia y rapidez a través de celulares y tablets en el mismo campo de trabajo.

Si bien el fenómeno de Big Data constituye un fenómeno global que puede llegar a tener un impacto económico real y potencial, beneficiando tanto al sector público y privado, en el aumento de la productividad, la competitividad sectorial y la calidad de vida de los ciudadanos[13].

En Argentina existe una alianza por los grandes datos entre el MINCYT y la Fundación Sadowsky, que presentaron una estrategia de utilización de grandes datos para Argentina en el periodo 2013-2018. Las industrias que más están avanzando con la implementación de Big Data son: Telco; media, entretenimiento, servicios y manufactura. En el caso de América Latina Argentina, Chile y Perú están avanzando, impulsados por los casos de uso de otras empresas pioneras en la región. "El tener ya casos de uso en países de Latinoamérica, empezando por Brasil, está permitiendo reducir el tiempo de adopción e implementación en los otros países, por lo que se empieza a ver un avance más veloz". Big Data surge como una nueva fase del paradigma intensivo en información y comunicación que abarca no sólo su dimensión tecnológica, sino también una dimensión social, económica, política y cultural[14].

Sin embargo estas nuevas oportunidades del Big Data van incrementando los riesgos y quizá el más relevante sea el que representa para la privacidad de las personas, con el tamaño y la complejidad legal también surgen una infinidad de retos en materia legal y normativa [2].

III. TITULARIDAD DE LOS DATOS

En su trabajo el Foro Económico mundial propone que a pesar de que los datos se refieran a individuos, se crean a partir de la interacción de diversas partes, de forma que todos ellos deben tener derechos y responsabilidades sobre esa información, los derechos deben ser comunes, no exclusivos [2]. Para responder al primer interrogante de quien son los

[3] https://www.foreignaffairs.com/articles/2013-04-03/rise-big-data

[4] http://www.redalyc.org/html/911/91145342001/

[5] Moreno, A., Redondo, T. (2016). Text Analytics: the convergence of Big Data and Artificial Intelligence. En International Journal of Interactive Multimedia and Artificial Inteligence

[6] http://searchdatacenter.techtarget.com/es./Definicion/Analisi-de-big-data

[7] www.mincyt.gob.ar/adjuntos/archivos/000/039/0000039687.pdf

[8] http://newsroom.cisco.com/press-release-contet-tipe-ebcontent-articled888280

[9] http://epic.org/privacy/big-data

[10] http://www.lavozdegalicia.es/noticia/mercados/2017/12/big-data-petroleo-SigloXXI

[11] http://searchdatacenter.techtarget.com/es/cronica/Solucion-de-federacion-de-datos-de-EMC-impulsa-implementacion-de-big-data

[12] http://www.pescar.org.ar/wp/s-i-r-v-e-datos-en-accion/

[13] Malvicino, Facundo, Joguel, Gabriel. Big Data Avances recientes a Nivel Internacional y particularidades en el Desarrollo local. Publicado en file:///E:/Descargas%20Marz%2017/ciecti-big-data-.pdf

[14] file:///E:/Descargas%20Marz%2017/ciecti-big-data-.pdf

datos, se debería esbozar que el titular de los recursos de computación debe poder probar de alguna manera que ha tomado las cautelas necesarias para garantizar la seguridad de sus sistemas en el ambiente de la integridad, confidencialidad y disponibilidad. Las normas de protección de datos [3] aseguran que los individuos son quienes tienen el control sobre la información que de ellos se incorporan a las bases de datos, el foco de atención ya no debe ser el momento de la recolección de datos, sino el momento de la utilización de sus datos.

¿Respecto del Segundo interrogante planteado en el sentido de porqué las empresas utilizan mis datos?, la legislación Argentina solo deja claro que es la empresa la que pone los medios para elaborar una base de datos, y quien tiene una serie de derechos sobre los mismos. Se debería hablar en términos de titularidad o más bien de uso en base a lo establecido en determinado acuerdo[15]. Dependiendo del tipo de dato del que se trate el criterio de acceso que se aplicara es disímil [4].

Entre los principales factores de riesgo se pueden mencionar:

A. Cámaras de Seguridad, Vigilancia.

La proliferación de dispositivos de video vigilancia, o los que utilizan a modo de soporte el propio cuerpo humano, como la biometría, y cuyo uso se extiende a terrenos cada vez más cotidianos y diversos como los utilizados para Defensa, seguridad e inmigración utilizados en los áreas de gobierno [5].

La captación de imágenes en la vía pública, no se agota en la conducta de algunos ciudadanos que captan imágenes con sus cámaras, sino que también abarca la utilización de imágenes captadas por empresas de seguridad privada y las pertenecientes a la vigilancia estatal, a las que también se suma la enorme cantidad de imágenes que genera la proliferación de drones.

Para efectuar el seguimiento de los movimientos de los compradores y dado que las señales de GPS no suelen percibir en el interior de las superficies de venta o ciertos comerciantes minoristas puedan utilizar otras tecnologías electrónicas. Estas tecnologías incluir RFID en los productos o en los carros de compra, cámaras de video y varias tecnologías innovadoras aprovechando los teléfonos móviles entre ellas el reconocimiento facial en los servicios en línea y móviles en Argentina y en resto de los países latinoamericanos no existe gran conciencia sobre el uso de datos biométricos. Estas videocámaras pueden ser excelentes para la gestión del flujo de tráfico, pero difíciles de utilizar para el seguimiento de la conducta de los individuos que entra en conflicto con la Ley de protección de datos, a no ser que las imágenes se distorsionen para impedir las identificaciones individuales.

Finalmente mencionaremos la Directiva 680/2016, del Parlamento Europeo y del Consejo relativo a las personas físicas destinados a los ámbitos policiales y a la justicia.

B. Datos Medicos

El Consejo de Europa ha señalado que los datos médicos forman parte de la esfera de intimidad de las personas, de manera que su trasmisión o divulgación solamente se pueden hacer en temas y problemas muy concretos y restringidos. Al respecto la Convención para la protección de los individuos en relación al tratamiento autorizado de datos personales, en su Art. 6 dispone que los datos personales relativos a la salud no puedan ser procesados automatizadamente, a menos que el ordenamiento nacional proporcione medidas de seguridad apropiadas. En ese sentido nuestra Ley 25326 nos ha brindado un estándar de puerto seguro al establecer que los datos vinculados a la salud solo podrán ser tratados, a fin de realizar oferta de bienes y servicios, cuando hubiesen sido obtenidos de acuerdo con los principios rectores establecidos por la misma ley y siempre que no causen discriminación. Estos datos no podrán ser transferidos a terceros sin el consentimiento previo, expreso e informado del titular de los datos quien deberá recibir una noticia clara del carácter sensible de los datos y de que no está obligado a suministrarlos, junto con su derecho de solicitar su retiro de la base de datos. El Reglamento de la Unión Europea sobre la Protección de datos publicado el 27/04/2016, estableció que el consentimiento debe ser "Libre, específico, informado e inequívoco".

Tal cual lo expresa[16] "Toda actividad medico asistencial tendiente a obtener, clasificar, utilizar, administrar, custodiar y trasmitir información y documentación del paciente debe observar el estricto respeto por la dignidad humana y la autonomía de voluntad, así como el debido resguardo de la intimidad del mismo y la confidencialidad de sus datos sensibles conforme la Ley 25326". Esto último se ve acentuado después de la reforma del Código Civil y Comercial de la Nación (C.C.C.), especialmente por los principios establecidos: Buena Fe (Art. 9), Abuso de derecho (Art.10), Abuso de la posición dominante (Art.11), Orden Público (Art.12) y Prohibición de renuncia de las Leyes.

Además hay que tener en cuenta la Ley sobre derechos del paciente Nº26529, que define en su art.5 el consentimiento informado como, "la declaración de voluntad suficiente efectuada por el paciente, o por sus representantes legales en su caso, emitida luego de recibir por parte del profesional interviniente información clara, precisa y adecuada" y Nº26742, Decreto 1089/2012 y el Art. 59 del CCC.

Finalmente también hay que tener en cuenta las Normas sobre Buenas prácticas Clínicas (GCP-ICH). La declaración de Helsinki y las disposiciones del ANMAT Nº5330/97, 690/05,1067/08,6550/08 Res BNº1490/07, La Ley 11044 y Decreto 3385/08 y lo Establecido por el Ministerio de Salud Mediante Decreto 3385/08 sobre consentimiento informado.

C. Servicios en la Sube

Conforme lo afirman los autores, el objetivo general de The Cloud, es entender los desafíos de seguridad, privacidad y confianza es aconsejar sobre las políticas y otras intervenciones que deben considerarse para garantizar que los

[15] http//:agaargentina.org/2015/10/08

[16] Iñiguez. Marcelo Daniel. Derecho de los pacientes. Revista de Derecho Privado y Comunitario. Pág.49- 91. Editorial. Rubinzal Culzoni.2011

usuarios europeos de entornos de nube cuenten con las protecciones apropiadas y para sostener un liderazgo europeo Nube. La computación en la Nube está cada vez más sujeta al interés de los encargados de formular políticas y de las autoridades reguladoras. La reciente Agenda Digital 1 de la Comisión Europea puso de manifiesto la necesidad de desarrollar una "estrategia nube" paneuropea que sirva para apoyar el crecimiento y el empleo y crear una ventaja de innovación para Europa. Sin embargo, la preocupación es que actualmente existen una serie de desafíos y riesgos en materia de seguridad, privacidad y confianza que pueden socavar el logro de estos objetivos políticos más amplios. Los autores citados precedentemente analizan además las complejidades tecnológicas, operativas y jurídicas del Cloud Computing, teniendo en cuenta la dimensión europea y los intereses y objetivos de todas las partes interesadas (ciudadanos, usuarios individuales, empresas, proveedores de servicios en la nube, autoridades públicas). Su estudio representa una progresión evolutiva en la comprensión de las implicaciones de la computación en nube para la seguridad, la privacidad y la confianza.

Las empresas líderes del sector han analizado en recientes publicaciones las amenazas y riegos del Cloud Computing y han efectuado recomendaciones. Sus preocupaciones se traslucen en aspectos como la gestión de datos, fundamentalmente en la propiedad de los mismos y la forma de operarlos y de tratarlos por parte de los proveedores, y en la identificación y control de acceso a los recursos. Además se incluyen refuerzos se seguridad en cuanto a la confidencialidad de los datos[17].

El Open Cloud Manifiesto establece una serie de principios para garantizar una nube abierta. Colaboración abierta y un adecuado uso de los estándares para hacer frente a los retos que ofrecen la implantación de la nube. Los proveedores de servicios no deben retener a los usuarios en determinadas plataformas impidiendo la libertad de elección. Cuando sea pertinente los proveedores deben utilizar los estándares vigentes. Los nuevos estándares que se adopten deben promover la innovación y en ningún caso restringirla[18].

Los líderes de datos y análisis ahora vienen de todas las partes del negocio[19]. Los programas de datos y análisis ya no son dirigidos exclusivamente por TI, sino que son creados por y para otros líderes empresariales. La naturaleza integrada, conectada y en tiempo real del negocio digital requiere la colaboración entre unidades organizativas históricamente independientes, y los programas de datos y análisis están en el centro de todo. Para darse cuenta de su visión de negocio digital y para la colaboración entre organizaciones, los negocios y las TI deben trabajar juntos en visión, estrategia, roles y métricas.

Tal cual lo afirmado[20] “las organizaciones que conformen alianzas para implementar una infraestructura cloud comunitario deberán tener objetivos similares y un marco de seguridad y privacidad común para resguardar la información corporativa, en este sentido la Cloud Security Alliance asiste a las organizaciones en la toma de decisiones y en la adopción e estrategias”.

IV. Privacidad

El Big Data desafía todas las normas de protección de datos al facilitar la re-identificación de los sujetos, ya no solo a partir de los datos pseudónimos, sino también a partir de datos que consideramos anónimos, y a ello podemos agregar que también pueden ser datos de carácter personal si consideramos el concepto amplio promovido por las normas comunitarias. Los datos sobre Salud que luego se anonimizan y se procesan para fines de investigación, dado que el Big Data incrementa la cantidad y diversidad de información, facilita la re identificación de individuos e incluso después de haber sido anonimizados[21]. Se han planteado algunos modelos que examinan los ataques de re-identificación que pueden realizarse en versiones que se adhieren al anonimato mientras se respeten las políticas de acompañamiento[22].

En este marco la Unión Europa ha publicado el Reglamento de la Unión Europea, sobre la Protección de datos, el 27/04/2016, que aunque es de aplicación directa en todos los estados miembros desde el momento de su publicación, ha establecido que comenzara a regir desde el mes de mayo de 2018. Allí se incluyen conceptos como la privacidad desde el diseño que exige que la privacidad se tome en consideración desde la fase inicial, desde el mismo diseño del producto o servicio, con ello no solo se conseguirá una mayor eficiencia en la protección de los derechos de los afectados. La inclusión de estos conceptos obligara a las empresas a actualizar sus procesos internos para adaptarlos a estos requerimientos además a partir de la aplicación de este Reglamento será obligatorio el informe sobre el impacto de privacidad en la intimidad.

Uno de los modelos propuestos, y que está siendo probado en países como Reino Unido, es la creación de permisos para el tratamiento de datos diferentes en función del contexto en el que se quieren utilizar (Por Ej. en el ámbito sanitario, el financiero etc. [2].

El concepto de huella digital ha generado innumerables debates y polémicas sobre lo que es información de identificación personal. Sin embargo se ha puesto de manifiesto una problemática porque se han encontrado huellas personales en datos que hasta entonces no habían sido considerados de identificación personal. Es decir, a pesar de que en una base de datos no aparezca nombres, se aprecian patrones y con estos patrones, una persona con suficientes conocimientos analíticos puede obtener nombres.

Las tecnologías de la información han generado un nuevo

[17] Guidelines on Security and Privacy in Public Cloud Computing .National Institute of Standards and Technologies (Nist)

[18] Ponencia CACIQ. Desarrollo de aplicaciones para Cloud Computing. María Murazzo1 , Nelson Rodríguez13, Daniela Segura2 , Daniela Villafañe

[19] Stefik, Mark. Internet Edge: Social, Technical and Legal Challenges for a Networked World. Cambridge, US: MIT Press, 2000. ProQuest ebrary. Web. 4 April 2017. https://mitpress.mit.edu/books/internet-edge

[20] 40 JAIIO-SID 2011.Becerra, María del Carmen, Navarro Mirtha Elizabeth. Cloud Computing: Seguridad y Protección de la confidencialidad de archivos digitales. ISSN: 1850-2814

[21] Kenneth Neil Cukier. Big Data: Revolution that will Transformation. https://www.hodder.co.uk/assets/.../Big%20Data%20first%20ch.p.

[22] https://dataprivacylab.org/dataprivacy/projects/kanonymity/kanonymity.html

concepto de identidad: la digital[6]. El perfil de la "persona virtual" se define en la red y se nutre de los contenidos que la misma proporciona respecto de un determinado individuo o compañía: la web otorga contenido, identifica e individualiza a la persona de una u otra manera.

Así, la identidad digital, representa las mismas características y actividades, que la identidad real, pero llevadas a cabo en internet, como consecuencia del crecimiento de las comunicaciones digitales. Esta identidad es la que se refiere como "vida virtual".

Algunos autores la conceptualizan, como "El conjunto de rasgos y características particulares, que una persona expresa a través de internet, forma una parte inescindible de la identidad personal de cada sujeto, en su faz dinámica, y más precisamente en su aspecto psicológico, social y moral".

La identidad digital se construye [6] de forma activa, aportando textos, imágenes y vídeos a Internet, participando, en definitiva, del mundo web. En los sitios de redes sociales, se construye a partir de un perfil de usuario, que a menudo se enlaza a perfiles de otros usuarios o contactos. En la identidad digital convergen muchos aspectos de carácter sociológico, cultural e incluso psicológico [7].

Para Benantar [8], es una representación de una entidad activa en la computadora. Dicha entidad puede ser física (usuario, servidor u otro dispositivo) o software. La identidad está asignada a un identificador el cual a su vez contiene atributos y derechos los cuales están referenciados a un perfil, un sistema de manejo de identidades pretende que la creación, asignación de derechos o negación de permisos de un perfil sea lo más sencillo posible. Por lo tanto se puede definir el manejo de la identidad como la administración de la misma, bajo estándares establecidos para que la seguridad de la información sea la correcta.

V. Modelo de Integración de guías, normas y estándares para la Gestión de Privacidad

En las industrias de la salud, servicios públicos y servicios financieros existen muchas guías de diversos reguladores, quizá no obligatorias, pero si altamente recomendadas. También existen estándares contractuales como el PCI y DDS que controlan la información de transacciones con tarjetas de crédito. Por último existen estudios de la industria para el seguimiento de la información publicada por organismos como el CERT (Computer Emergency Response Team) y las familias de estándares ISO.

Se parte de realizar una búsqueda en los documentos publicados hasta el momento, se ve que el proceso de autenticación de identificación biométrica se basa en las normas ISO/IEC 17.799, 27.001 y 27.002 (estándares centrados en la seguridad de la Información), COBIT (estándares centrados en la gestión), ITIL (estándares centrados en los organismos públicos), y ANSI NIST-ITL 378 (estándares centrados en la seguridad de datos biométricos).

Las Normas IRAM ISO/IEC 27.001 y 27.002, definen y documentan, los roles y responsabilidades de la seguridad de los empleados, contratistas y terceros en concordancia con la política de seguridad de la información de la organización. Garantizan la protección y privacidad de los datos según lo requieran las legislaciones y si fueran aplicables, las clausulas relevantes contractuales.

Existen además, normas como la ISO 24.760 e ISO 29.100, que proporcionan un marco de referencia de alto nivel para la protección de los datos personales, y regulan la Gestión de identidad y Privacidad. Aportan a la gestión de privacidad las ISO29134, e ISO 29151, ISO 29190/91 que presenta un modelo de evaluación de la capacidad en privacidad. La norma ISO / IEC 27018: 2014 establece objetivos de control comúnmente aceptados, controles y guías para implementar medidas para proteger la Información de Identificación Personal (PII) de acuerdo con los principios de privacidad en ISO / IEC 29100, para el entorno de computación en nube pública. En particular, especifica directrices basadas en ISO / IEC 27002, teniendo en cuenta los requisitos reglamentarios para la protección de las IIP que podrían ser aplicables en el contexto del entorno de seguridad de la información de un proveedor de servicios públicos servicios en la nube. Es aplicable a todos los tipos y tamaños de organizaciones, incluyendo empresas públicas y privadas, entidades gubernamentales y organizaciones sin fines de lucro que proveen servicios de procesamiento de información como procesadores PII a través de Cloud Computing bajo contrato con otras organizaciones. Estas directrices también podrían ser pertinentes para las organizaciones que actúan como controladores de PII; Sin embargo, los controladores de PII pueden estar sujetos a leyes, reglamentos y obligaciones adicionales de protección de PII, que no se aplican a los procesadores PII. ISO / IEC 27018: 2014 no pretende cubrir tales obligaciones adicionales.

COBIT Acrónimo de "Control Objectives for Information and Related Technology" (Objetivos de Control para la Información y Tecnologías Relacionadas), es un estándar desarrollado por la Information Systems Audit and Control Foundation (ISACA). Se destaca el rol de COBIT 5 en la estrategia de seguridad y objetivos de control, en el nuevo marco para la gobernanza en TIC´S, y guías de COBIT 5 sobre seguridad y riesgo. Los Estándares ANSI/NIST-ITL son estándares que se aplican internacionalmente para proteger los datos biométricos. El propósito de esta norma es que un sistema biométrico dactilar pueda realizar procesos de verificación de identidad e identificación, empleando información biométrica proveniente de otros sistemas.

En el modelo de la selección de estándares y normas, se utiliza el método de estudio de comparación de los mismos, se crean plantillas para la comparación de las similitudes respecto a la gestión de la identidad y la privacidad. El modelo aplico la evaluación de normas y estándares, que proporcionan una base sólida para el cumplimiento de los objetivos de la Organización, en cuanto a la seguridad de los datos personales. Se basó en los modelos que tienen más fortalezas en la relación a la gestión de capacidad de servicio de TI, son el modelo ITIL [9] y las Normas ISO/IEC 27.001 y 27.002 que permiten que la información y la tecnología relacionada se rijan y se gestionen de manera integral en toda la empresa [10].

Es un modelo de integración[23] donde las normas y estándares a ser evaluados responden a un modelo general de valuación de los sistemas de información, como conjunto de

[23]http://wwwsedici.unlp.edu.ar /handle/10915/56368

elementos interrelacionados para lograr un objetivo específico. En el modelo general se evalúan las normas y estándares de seguridad, en primer lugar se detectó el estado del arte de las normas y estándares, luego se las comparó en función del uso e impacto de cara al ciudadano, de cara al empleado y de cara al usuario. En el Modelo de integración de estándares[24] se midió el impacto desde tres perspectivas y la eficacia mediante el cumplimiento del principal objetivo que es la seguridad. Este análisis se hace previo a su implementación, formulando criterios de evaluación que permiten ponderar su importancia en la protección de la privacidad.

VI. MODELO DE PRIVACIDAD

Son necesarios los mecanismos de legalidad internacional, por lo riesgos que el Big Data supone para la privacidad, esto ha hecho cambiar el foco de atención, ya no se debe cumplir solo con los principios de protección de datos ahora se debe tener en cuenta la privacidad desde el mismo modelo de negocio, es decir que la privacidad deja de ser un concepto legal para ser una prioridad del negocio.

Dado que el modelo de Evaluación del impacto sobre la protección de datos no está suficientemente avanzado y desarrollado, pero es una primera aproximación que se genera desde el proyecto referenciado[25], está en proceso de contratación y es un presupuesto necesario para brindar a los responsables del tratamiento una orientación práctica suficientemente específica, útil y clara.

Las Organizaciones desarrollan un conjunto de actividades y procesos, que deben gestionarse sistemáticamente de tal forma que permitan el cumplimiento de sus objetivos [11]. Esto conduce al equipo de trabajo a pensar que los SI necesitan de una visión y una evaluación interdisciplinaria. En este sentido, aparece una nueva perspectiva definida como Artefacto SI que tiene como componentes: el Artefacto TI, su Uso y su Impacto [12].

El modelo del que se coteja como genérico se ha denominado ***Modelo de las 5 vocales*** (Figura 1). *Este toma como referencia la teoría del Éxito de William DeLone y Ephraim McLean. En este se enfatiza el uso y el impacto de los SI, como así también pone principal esmero en la satisfacción del usuario y sus beneficios netos, considerando que la calidad del sistema está en relación directa con estas variables (Delone, McLean, 2003) De esta forma todos los artefactos de Tecnologías de Información (TI), en la mayoría de los casos representados por proyectos de software, normalmente evaluados mediante métricas específicas, requieren de una perspectiva desde las diferentes ciencias.*

La nueva normativa europea obligara a las empresas a realizar la evaluación de impacto fijando una serie de criterios para su realización [13].

De esta forma todos los artefactos TI, en la mayoría de los casos representados por proyectos de software[14], los que generalmente son evaluados mediante métricas específicas, requieren de una perspectiva desde las diferentes ciencias, lo que nos lleva a pensar que los SI necesitan de una visión interdisciplinaria[15].

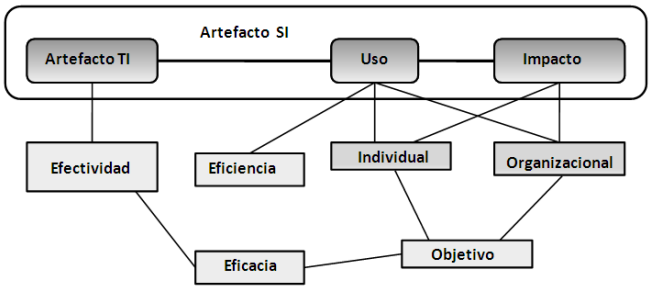


Fig. 1. Modelo General

La incorporación del Objetivo individual y organizacional y conceptos como el de efectividad que se basa en la eficacia (cumplimiento de Objetivos) y la Eficiencia (relación insumo/producto) pretende realizar una representación de los sistemas de Información desde la perspectiva de su análisis cuantitativo y cualitativo.

Se adoptan los siguientes criterios propuestos en otros informes y trabajos de la Agencia de Protección de datos Española, GT29:[26] 1) La relación entre el fin que se tomaren los datos y el fin del Modelo actual, 2) El contexto en el que se obtuvieron los datos y las expectativas de los sujetos, 3) La Naturaleza de los datos y su posible impacto, 4) Las medidas de salvaguarda que se aplican como la imposición de condiciones de uso de los datos cuando estos se cedan a terceros. Además se realiza un reconocimiento explícito del concepto de Privacidad por diseño y Privacidad por defecto. También la solución que propone es la aplicación de un modelo de "ética de la privacidad"[27].

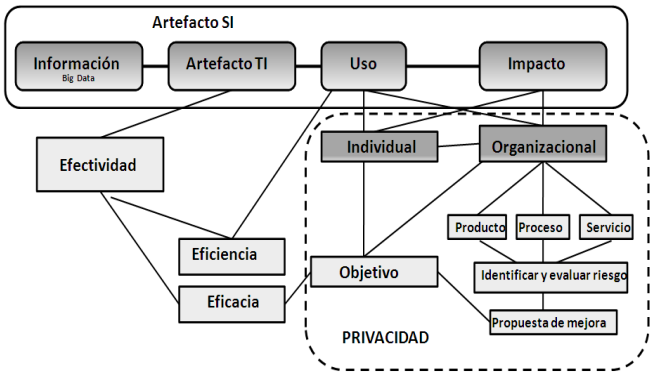


Fig. 2 Modelo de Privacidad

Con este trabajo se pretende brindar un modelo (Figura 2)

[24]Becerra, María del Carmen, Zarate Pedro, Gómez Claudia. Modelo de integración de Estándares para la Gestión de Identidad y Privacidad. XXII Cacic2016. (WSI). Workshop de Seguridad Informática. UNSL.
http://sedici.unlp.edu.ar/handle/10915/56368

[25]Proyecto de Investigación "Representación genérica de modelos conceptuales en el campo de los Sistemas de Información" FCEFN-UNSJ

[26] http://wwww.agpd.es/.../index-ides-idphp

[27]https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/premios_2015/Big_Data_Privacidad_y_proteccion_de_datos.pdf

para que las organizaciones tanto públicas como privadas puedan gestionar la seguridad de la privacidad de los datos sensibles, con el fin de fortalecer la protección de datos conforme los estándares vigentes. Un nuevo modelo de negocio es planteado basado en ese empoderamiento de los individuos, el Foro Económico Mundial propone dos fases para desarrollar el nuevo modelo. La primera fase basada en esta creación de permisos diferenciados en función del contexto, la segunda fase consiste en la gestión de la información, lo que implica un cambio de paradigma en la gestión de los datos respecto de los modelos actuales.

De esta manera se pone el foco de atención en el uso de los datos y no sobre la recolección, se pretende otorgar un papel más relevante (y de mayores responsabilidades) a las empresas y organismos que vayan a hacer uso de los datos. La ventaja fundamental será permitir medir la efectividad y la eficiencia, teniendo en cuenta la eficacia y como se usa e impacta sobre la privacidad [15].

La privacidad plantea riesgos que deben ser bien gestionados profesionalmente de una manera similar a la categoría de riesgos. Las organizaciones que manejan datos de carácter personal deben supervisar sus procesos en curso, ya que están tratando con datos de clientes, empleados o el público en general y esos tratamientos pueden afectar derechos fundamentales [16].

VII. Conclusion

En este trabajo se combina la experiencia de diferentes áreas del proyecto para dar información valiosa sobre lo que los grandes datos están haciendo, lo que puede hacer y lo que se debe permitir hacer [17].

El aumento de la regulación y la legislación sobre la privacidad también está impactando en los entornos TI [18]. La adopción de modelos y normas facilita la rápida ejecución de los buenos procedimientos y ayuda a evitar retrasos innecesarios en el desarrollo de nuevos enfoques [19]. Todas las empresas tendrían que adaptarse al uso de modelos y establecer normas para ajustar sus requisitos individuales [20].

Cada organización debe establecer su propia estructura de gestión y recoger en todos ellos las recomendaciones que resulten más útiles. El uso de estándares ayuda al cumplimiento de las leyes, reglamentos, acuerdos contractuales y políticos y a ganaren ventajas competitivas sobre otras organizaciones [16].

El modelo genérico presentado para la gestión de privacidad de grandes datos Big Data permitirá la definición de modelos más específicos según el contexto en que sean usados los datos[28].

VIII. Referencias

[1] Joyanes, L. Big data: análisis de grandes volúmenes de datos en organizaciones. Barcelona: Marcombo. Ediciones Técnicas 2014. http://www.marcombo.com/Big-data_isbn9788426720818.html

[2] Gil González, Elena. Big Data-Privacidad y Protección de datos. Madrid 2016.

[3] Bueres Alberto, Código Civil y Comercial de la Nación analizado, comparado y concordado. 1ra Ed. Bs. As. Ed. Hammurabi. 2014.

[4] Navarro Mirtha, Becerra, María del Carmen. Gestión Integral de Infraestructuras Criticas en las Organizaciones Locales alineados a las Normas IRAM ISSO 27.001 y 27002. WSI - II Workshop de seguridad informática CACIQ 2013.

[5] Borghello Cristian, Temperini Marcelo G. 41 JAIIO. Suplantación de Identidad Digital como delito informático en Argentina. (Online).2012. www.41jaiio.sadio.org.ar/sites/default/files/7_SID_2012.pdf

[6] La gestión de la identidad digital: Una nueva habilidad informacional y digital. BID. Universidad de Barcelona http://bid.ub.edu/24/giones2.htm 2010.

[7] http://blog.segu-info.com.ar/2012/07/como-se-construye-una-identidad-digital.html.2012.

[8] Benantar, M.Access Control Systems-Security-Identity Management and trust Models New York: Springer. 2006.

[9] Alleinni Féliz-Sánchez, José Antonio Calvo-Manzano. Comparison of models and standards for implementing IT service capacity management. 2015. www.redalyc.org/pdf/430/43038629008.pdf

[10] El derecho informático y la gestión de seguridad de la información una perspectiva con base a la norma ISO 27001. Revista del Derecho. Biblioteca de Ciencia y Técnica de la Nación 2008.

[11] Jacobson, I; Booch, G; Rumbaugh, J. El proceso unificado del desarrollo de software. Pearson 2000.

[12] DeLone, W, McLean, E., "Model of Information Systems Success: a ten years update". Journal of Management

[13] https://www.masprivacidad.com/2017/03/01/la-privacidad-en-el-dise%C3%B1o-y-por-defecto/

[14] Gonzalo Pérez-Tomé Estévez. Estudio sistemático de literatura de metodologías para la obtención de requisitos de privacidad. 2015. http://www.dit.upm.es/~posgrado/doc/TFM/TFMs2014-2015/TFM_Gonzalo_Perez-Tome_Estevez_2015.pdf

[15] Diana M. Castillo Pinzón, DM. Enfoque para combinar e integrar la gestión de sistemas. 2010.

[16] Burgos Salazar, Jorge; Pedro G. Campos. Modelo para Seguridad de la Información en TIC. http://ceur-ws.org/Vol-488/paper13.pdf 2017.

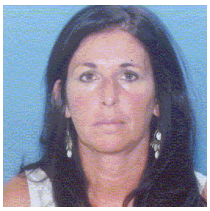
[17] Moreno, A., Redondo, T. Text Analytics: the convergence of Big Data and Artificial Intelligence. En International. Journal of Interactive Multimedia and Artificial Intelligence. 2016.

[18] Neil, Robinson. Cloud: Understanding the Security, Privacy and Trust Challenges. RAND Corporation 2011.

[19] Information Systems / spring 2003, Vol. 19, No. 4, pp. 9–30. © 2003 M.E. Sharpe, Inc. 0742–1222 / 2003.

[20] Arce Iván. Seguridad Tic. Desafíos y oportunidades para emprendimientos de base tecnológica en Argentina. Fundación Dr. Manuel Sadosky 2014.

[28]http:///ec.eropa.eu/rewroom/just/item-detaib.cfm?item.ide-50083



María del Carmen Becerra, Autor nació en Argentina provincia de San Juan. Se recibió de Abogada en la UCC, en 1990. Magister en Informática en la Universidad de la Matanza 2007. De 2008 hasta el presente es Docente Investigador de la Facultad de Ciencias Exactas, Físicas y Naturales de la Universidad Nacional de San Juan- Es autor de más de 50 artículos publicados. Sus intereses de investigación incluyen temas de Derecho Informático e Informática Jurídica en su estrecha relación con los SI y TICs. Integra el Proyecto Representación Genérica de modelos conceptuarles en el campo de los sistemas de Información. Donde ha realizado publicaciones en la 44 JAIIO 2015, sobre Intimidad y Privacidad en entornos digitales luego de la reforma del Código Civil. Y en el XXII CACIC 2016 del trabajo titulado "Modelo de Integración de Estándares para la Gestión de Identidad y Privacidad". Actualmente dirige el proyecto de investigación Representación Genérica de modelos conceptuarles en el campo de los sistemas de Información. Anteriormente ha dirigido el Proyecto "Identificación de Modelos Conceptuales en el Campo de los Sistemas de Información" Las presentaciones en congresos realizadas hasta la fecha son: "Un Modelo de Artefacto" SI. CONAIISI 2016, "Teorizando en SI". SABTIC 2016. "Modelo Genérico para Representar Sistemas de Información". SABTIC 2016. "Herramientas para generar contratos electrónicos en entornos de comercio electrónico basado en ontologías" JAIIO 2016. "Modelo de Integración de Estándares para la Gestión de la Identidad y Privacidad" CACIC 2016. "La Modelización Conceptual como Herramienta para Formalizar Sistemas de Información" JATIC 2016.

María Claudia Gómez, Autor nació en Argentina, provincia de San Juan. Se recibió de Licenciada en Administración de Empresas. (UNSJ, 1984) · Técnico en Investigación Operativa. (ESIO, 1977) · Licenciado en Investigación Operativa. (ESIO, 1978). - De Posgrado: Magister en Logística (UNCU, 2007), es profesor en el Departamento de Informática de la Facultad de Ciencias Exactas Físicas y Naturales de la UNSJ desde el año 1985 hasta la fecha. Es autor de numerosos trabajos que han sido publicados a nivel nacional e internacional. Sus intereses de investigación versan sobre: Sistemas de Información. Modelos. Metamodelos. Ontologias.

Pedro Daniel Zarate, Autor nació en Argentina provincia de San Juan. Se recibió de Programador Universitario en (UNSJ, 94). Procurador (UES21, 15). Desde 1989 a la fecha es Docente/ Investigador de la Facultad de Ciencias Exactas, Físicas y Naturales de la Universidad Nacional de San Juan, coordina el Laboratorio de Informática Forense e Informática Jurídica. Integra el Proyecto "Ideas en tiempo real, una plataforma tecnológica para la generación de ideas de productos Tecnológicos". Ha realizado publicaciones en la 44 JAIIO 2015, sobre Intimidad y Privacidad en entornos digitales luego de la reforma del Código Civil. Y en el XXII CACIC 2016 del trabajo titulado "Modelo de Integración de Estándares para la Gestión de Identidad y Privacidad.