Cloud Computing: Seguridad y Protección de la confidencialidad de archivos digitales.

Mag. Abogado María del Carmen Becerra[1]

Mag. Mirta Elizabeth Navarro [2]

Proyecto "Convergencia de Tecnologías informáticas y Metodologías para la implementación de sistemas de información"

Abtract: En este trabajo se plantea la redacción de normas y procedimientos que fijen buenas prácticas de seguridad; tanto para el control acceso a los recursos, como para la guarda de información confidencial o secreta, como única solución para los problemas legales que plantea el modelo Cloud Computing[3]. También para disminuir o limitar la responsabilidad civil y penal de las organizaciones. Cualquiera sea la infraestructura cloud que se contrate (redes, servidores, almacenamiento, aplicaciones y servicios) será imprescindible gestionar los riesgos de seguridad y para ello deberá identificárselos y valorárselos. Las organizaciones deberán definir contractualmente al propietario de los datos y determinar quien será el encargado de operarlos y tratarlos, conforme los parámetros que fija la legislación vigente para la protección de datos personales y tanto los proveedores como los usuarios deberán coincidir en las estructuras organizacionales que diseñen para enfrentar los incidentes de seguridad derivados de las tecnologías compartidas.

Palabras claves: Cloud computing. Seguridad en el Cloud. Amenazas riesgos y recomendaciones. Aspectos contractuales. Buenas prácticas en la gestión del riesgo.

1.-Introducción:

[1] Abogado, egresado de la UCC. Magíster en Informática egresado de la Universidad Nacional de la Matanza. Docente Investigadora de la U.N.S.J. Directora del Instituto de informática del Foro de Abogados de San Juan

[2] Licenciada en Administración de empresas egresada de la U.N.S.J. Magíster en Gestión de Organizaciones egresada de la Universidad de Valparaíso.Chile. Docente de la U.N.S.J. Directora del Proyecto Convergencia de Tecnologías informáticas y Metodologías para la implementación de Sistemas de información

[3] Peter Mell, Tim Grance, The NIST Definition of Cloud Computing, Version 15,October 7, 2009, URL: http://csrc.nist.gov/groups/SNS/cloud-computing. Modelo para hacer posible el acceso a red adecuado y bajo demanda a un conjunto de recursos computación configurables y compartidos (por Ej: redes, servidores, almacenamiento, aplicaciones y servicios) cuyo aprovisionamiento y liberación puede realizarse con rapidez y con un mínimo esfuerzo de gestión e iteración por parte del proveedor del cloud.

La tendencia indica que cerca de un tercio de las organizaciones en Latinoamérica[4] usarían el cloud a partir del año 2010, de esta manera las empresas buscarán escalar posiciones rápidamente en función de sus necesidades, sin tener que añadir equipamiento, software ni personal especializado. Sin embargo, si bien esto repercute en el ahorro de costes tanto económicos como operacionales, ello también genera múltiples riesgos para las organizaciones tomadoras del servicio por la trascendencia económica que adquiere la información en el patrimonio de las organizaciones modernas, ellas deberán tener un conocimiento preciso sobre el Cloud computing y su seguridad.

Coinciden los autores[5] que si bien Cloud Computing posee muchas ventajas, quizás la desventaja más importante es la pérdida de control sobre las aplicaciones y los datos, en cuanto a su manipulación y ubicación. Los problemas derivados de las tecnologías compartidas en los modelos de infraestructura como servicio exigen estrategias de seguridad para gestionar correctamente los recursos de manera que la actividad de un usuario no pueda interferir en las del resto. [6]

En nuestro país Conforme las políticas de clasificación y tratamiento de la información, establecidas en el ámbito nacional[7] los propietarios de la información deberían analizar la información a su cargo y proceder luego a su clasificación para autorizar expresamente su conservación, envío, impresión, divulgación a terceros y destrucción. Basándose principalmente en los perjuicios que pudiera ocasionarle al organismo y/o personas, el incumplimiento de alguno de los valores generales de seguridad definidos en la política de seguridad de la información adoptada por la organización.

Partiendo del concepto de que la seguridad de la información es inherente a la ética y a la función de las instituciones oficiales, la definición, medición y asignación de responsabilidades para el tratamiento de la información secreta debería ser ejecutada de forma ética. Los principios, convenciones, normas y mecanismos adoptados, deberían tener en cuenta las consideraciones y puntos de vista de todas las partes interesadas[8].

---

[4] Encuesta de ISACA IT Risk. Año 2010.En http://seguridad-informacion.blogspot.com/2010/05/encuesta-de-isaca-america-latina-adopta.html

[5] http://www.inteco.es

[6] Es un modelo en el cual la infraestructura básica de computo (servidores, software y equipamiento de red) es gestionada por el proveedor como un servicio bajo demanda, en el cual se pueden crear entornos para desarrollar, ejecutar y probar aplicaciones. http://csrc.nist.gov/gropus/SNS/cloud-computing.

[7] Políticas de seguridad de la Información dispuesta por la ONTI y adoptada en Argentina por Decisión Administrativa 669/2002 y Resolución SGP 45/2005. www.arcert.gov.ar/politica/PSI_Modelo

[8] Becerra, María del Carmen. Metodología de seguridad para el tratamiento de la información del proceso penal. SIE 2008.37 JAIIO.

En este trabajo se sostiene que los nuevos tipos de contratación[9] exigen que ambas partes asuman sus responsabilidades de una manera distinta a los postulados tradicionales de la responsabilidad civil, la previsión de antemano de las distintas cuestiones que plantea el modelo cloud computing exigen un deber de mayor de información por parte del proveedor del servicio[10] y un deber de decisión del usuario respecto a la implementación de medidas de seguridad y de buenas practicas[11] para el resguardo de la información que podría ser equiparada a la diligencia exigida para un buen hombre de negocios.

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[12] asiste a las organizaciones en la toma de decisiones y en la adopción e estrategias.

El Open Cloud Manifesto 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[13].

La provisión de servicios en la Cloud se encuentra en manos de unas pocas empresas y se estima que en un futuro no muy lejano esta cantidad será menor y se circunscribirá a los cinco grandes proveedores actuales (Sun - hoy Oracle-, Google, Microsoft, Amazon, IBM). Los autores opinan que si bien no es probable que exista un monopolio, si existirán proveedores hiperconsolidados y lideres en la provisión de servicios en la cloud. De lo que si podemos estar seguros es que esto generará que el usuario posea una fuerte dependencia del proveedor de servicios.

2.-Seguridad en el Cloud: Amenazas, riesgos y recomendaciones

[9] Almark, Daniel Ricardo. El contrato de Outsourcing de Sistemas de Información. Bs.As. Lexis Nexis. Argentina 2006
[10] Ley N° 26.361(B.O. 7/4/2008)
[11] NORMA IRAM ISO IEC 17.799.
[12] Informe “top Threarts to Cloud Computing” V 1.0” sobre las siete amenazas de la infraestructura cloud https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf
[13] Ponencia CACIQ. Desarrollo de aplicaciones para Cloud Computing.María Murazzo[1], Nelson Rodríguez[13], Daniela Segura[2], Daniela Villafañe[2]

Las empresas líderes del sector[14] 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.

La gestión de servicios en la nube provoca que el Usuario pierda el control sobre la gestión de la seguridad siendo necesaria la implantación por el Proveedor y por el Usuario de medidas dirigidas a proteger la integridad y confidencialidad de los datos y de la información. Se plantea como solución jurídica la Garantía de implantación de las medidas de seguridad por parte del Proveedor a nivel contractual y la redacción de un documento de seguridad[15] en función de los compromisos adquiridos en el contrato por cada parte. Además es recomendable que se acrediten certificaciones de cumplimiento de normativa (IRAM-ISO IEC 17799), sin embargo ello no es censillo cuando la evaluación del cumplimiento de los estándares queda arbitrariamente en manos de una de las partes[16].

Para algunos doctrinarios la puesta a disposición de la información al Proveedor de servicios constituye un tratamiento de datos por terceros y ello puede dar lugar a una cesión inconsentida de datos. Por ello se debería redactar de un contrato con proveedor del Cloud donde se especifique quien será el encargado del tratamiento de los datos, donde se efectuará el mismo y que legislación será aplicable.

La deslocalización de los servicios pueden dar lugar a transferencia internacional de datos no autorizadas por la Ley 25.326[17], las organizaciones deberán tener en cuenta si se traslada información a servidores ubicados en el extranjero o si se produce acceso a la información de países extranjeros, una solución estaría dada cuando la transferencia se realiza a países con nivel de protección adecuado[18] y formalizar un contrato para tal transferencia, sin embargo esto no sería aplicable en la actualidad dado que las empresas que se perfilan como proveedores líderes en la provisión de servicios Cloud se rigen por legislación extranjera y bastaría con mencionar como ejemplo las previsiones del Acta

[14] Guidelines on Security and Privacy in Public Cloud Computing . Nacional Institute of Standards and Tecnologías (Nist)

[15] NORMA IRAM ISO IEC 17.799.
[16] Almart, Ricardo .Obra Citada.
[17] Ley 25326 (B.O. 02/11/2000)
[18] Brenna, Ramón Jerónimo. Internet y privacidad. Reflexiones sobre la sociedad de la información y la recolección de datos on-line. Informática y Derecho. Aportes de doctrina internacional. Lexis Nexis. Desalma Bs.As. 2002-

Patriótica de EE.U.U[19], para comprender como se trata de evitar cumplir con las normas de orden público del lugar donde se encuentra el usuario.

Las amenazas internas descriptas en el informe "Top Threats to Cloud Computing"[20] constituyen la actividad que realizan los propios usuarios que tienen acceso natural a los datos y aplicaciones de la empresa, se pueden mencionar los numerosos incidentes de seguridad provocados por los propios empleados descontentos y los accidentes que suelen ocurrir por error o desconocimiento[21]. En este sentido se recomienda a las organizaciones incluir en los contratos cláusulas legales y de confidencialidad en los contratos laborales, sin embargo a veces es el propio proveedor del servicio el que gestiona las altas y baja de los usuarios, produciéndose brechas de seguridad cuando el consumidor del servicio no informa al proveedor de las bajas de personal de la empresa.

Una de las principales amenazas informadas por la CSA[22] es el secuestro o cesión del servicio, acá hay que destacar las amenazas que surgen en la nube cuando un atacante obtiene las credenciales del usuario para acceder a actividades y realizar transacciones para manipular datos y devolver información falsificada o redirigir a los clientes a sitios maliciosos, además la fuga o pérdida de información, también es una realidad en las empresas locales en el proyecto "Contribuciones al desarrollo de sistemas de información e implementación de las tecnologías de la información y comunicación en organizaciones locales"[23] quedo demostrado que en numerosas oportunidades los datos pueden ser borrados o modificados sin tener copia de seguridad de los originales. En la nube este riesgo aumenta ya que las interacciones entre los datos se multiplica y ello deriva no solo en daños a la compañía (demandas de los propietarios de los datos personales por infracción a la Ley 25.326), perdida de imagen de la compañía e incluso desaparición de la misma si se revelaran[24]los datos que hacen al Know How de la empresa.

Las metodologías de control de acceso de la Norma IRAM ISO IEC 17799[25] ayudan al control de acceso y mediante el cifrado de los datos secretos se podría proteger su tránsito[26].

[19] Otorga amplios poderes especiales al FBI y a las agencias de inteligencia de EEUU para poder monitorear el trafico del correo electrónico
[20] https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf
[21] http://www.mundo-contact.com/enlinea_detalle.php?recordID=21377
[22] Cloud Security Alliance
[23] Proyecto de Investigación de la U.N.S.J.
[24] Por Ej.: mediante los hipervisores de virtualización los recursos físicos el anfitrión
[25] Norma IRAM ISO IEC 17799. Punto 5.2.1 Pautas de clasificación de la información
[26] Ley de firma digital 25506 (B.O. 14/11/2001)

Otro de los riesgos mencionados en el informe es de riesgos por desconocimiento por lo que para la toma de decisiones sobre las medidas de seguridad que se han de implementar en las organizaciones, es necesario conocer información técnica de la plataforma, sobre con quién se comparte la infraestructura y sobre los intentos de acceso no autorizado. Sin embrago los proveedores de servicio son reticentes a brindar esta información respecto de sus políticas de seguridad y privacidad argumentando que dicha información podría ser utilizada para un ataque.

3.-Aspectos contractuales a considerar:

La realidad de la nube nos muestra que las empresas proveedoras de servicios utilizan el Contrato de adhesión, donde la mayoría de las cláusulas revisten el carácter de predispuestas, sin embargo el receptor de los servicios debería tratar de equilibrar los riesgos que supone la utilización del servicio. En la medida en que los servicios se vayan haciendo más complejos las partes deberían negociar un contrato a medida y asegurarse de que el contenido del contrato se ajusta a sus necesidades durante su vigencia. Además en el momento de la resolución deberá contar con los mecanismos correspondientes que permitan la minoración de los riesgos.

En la redacción por vía contractual de las condiciones en las que se va a llevar a cabo el control por parte del Proveedor (la actividad laboral, como del adecuado uso de las aplicaciones), se deberá aplicar la Proporcionalidad y evitar los medios intrusivos injustificados. Además se deberá prever a modo de creación, las evidencias electrónicas mediante procedimientos de conservación y aportación.

Si bien se pueden mencionar múltiples aspectos a considerar en la etapa precontractual se analizarán los siguientes:

- Calidad del Servicio
- Ubicación física del hardware y del software utilizado problemas de jurisdicción y competencia.
- Características de seguridad. Detalles de la red y monitorización del servicio.
- Manejo de los datos personales: ¿El proveedor entrega los datos a terceros?
- Sub contratación en cloud computing
- Protección de datos: confidencialidad, integridad y disponibilidad de los datos

- Garantizar a través de anexos técnicos la protección de la custodia de la información que le suministra el cliente, medidas de seguridad como acceso restringido, limitación de copia de la información

- Cláusulas de confidencialidad

- Cláusulas de responsabilidad por el mal manejo de los datos

Cláusulas más habituales-Modelo Contractual

Alcance de los Servicios. Autorización para el Uso del Servicio En muchas ocasiones se cede el servicio en su conjunto, no las aplicaciones que forman parte del mismo. Es función del Proveedor la Identificación del prestador del servicio, es decir si van a ser prestados directamente por el proveedor o si van a ser prestados por terceros. En ese caso habría que determinar que parte de los servicios van a ser prestados por esos terceros y habría que informar la cesión a terceros del Contrato.

Usuarios Tipos: Usuarios Principales. Usuarios Finales: Pertenecientes a la organización. El Usuario Principal y dependientes del mismo. Requisitos: Titularidad de la Cuenta. Nombre de Usuario. Contraseña. No tener la condición de competidor. No pertenencia a jurisdicciones donde los servicios se encuentren prohibidos.

Condiciones de Uso del Servicio Finalidades a la que va destinarse la información alojada en la nube Responsabilidades respecto de la gestión de la Información Prohibición del Usuario de alterar el Servicio y usar la información que pudiera suministrar el proveedor Confidencialidad Finalidades autorizadas Posibilidad de revender y sublicenciar el Servicio Cesiones a terceros Condiciones relativas a la exportación de servicios y productos

Monitorización Dadas las características de la prestación del servicio, fuera del control del cliente, y su forma de pago, pago en función del uso es muy importante reflejar de un modo claro los términos del cumplimiento uso, Es necesario reflejar, la facultad del Usuario para poder monitorizar el funcionamiento del servicio y de este modo poder comprobar lo siguiente: Las medidas de seguridad necesarias, los controles y las políticas dirigidas a garantizar la integridad de los datos.

Contenido: Los procedimientos de gestión ante posibles incumplimientos y las sanciones a imponer en caso de incumplimiento: Personas de contacto Plazos Modo de descripción de los incidentes Criterios de validación de las incidencias. Los mecanismos de compensación establecidos para los casos de incumplimiento:

Penalizaciones Créditos, abonos de servicio. Actuaciones dirigidas a la subsanación de los incumplimientos

Los servicios objeto de prestación por parte del proveedor. Instrumentos a emplear para poder medir el cumplimiento del servicio[27] y los recursos utilizados por el usuario. El nivel de disponibilidad y las circunstancias controladas o no que pueden dar lugar a la falta de de cumplimiento del nivel de servicio pactado. Servicios no comprendidos Situaciones fuera del control del prestador de servicios: Casos de Fuerza Mayor Problemas relacionados con las redes de telecomunicaciones Paros programados. Tener en cuenta que se va a producir cierta escalabilidad en la asignación de recursos y que durante los procesos de escalado se producen incumplimientos es preciso determinar cuales son los parámetros que se van a tener cuenta durante esas fases a la hora de valorar si se ha producido la efectiva prestación de los servicios.

Suspensión del Servicio: Se deben tener en cuenta las siguientes circunstancias: Usos indebidos del servicio Impagos Emergencias en materia de seguridad Paros programados Duración de la suspensión Condiciones del Levantamiento: Plazo: Consecuencias de sobrepasar el mismo Subsanar ó Subsanación de la circunstancia motivadora. Condiciones económicas: Tarifas respecto de los servicios que se siguen utilizando Posibles tarifas de reconexión

Resolución: Las Causas pueden ser: Finalización Plazo de vigencia Resolución Amistosa .Requisitos Notificación Cierre cuenta del Usuario Impagos Violación de las condiciones del servicio Usos fraudulentos de la cuenta Daños al sistema Quiebras, situación de concurso: Recomendable establecer mecanismos contractuales que permitan ó al Usuario poder recuperar la información. El cumplimiento con todas las obligaciones legales y normativas que resulten de aplicación. Es habitual cierto relajamiento en cuanto al cumplimiento de las mismas durante estos periodos de transición.

Consecuencias de la Resolución Cese de los derechos otorgados Devolución de la información Plazo Modo Formato Condiciones económicas Destrucción de la Información si se ha solicitado por el Usuario y si se dan determinadas circunstancias si se permitirá la conservación de la Información por el Prestador de Servicios: Con carácter previo a la devolución: Condiciones económicas Una vez devuelta la misma al Usuario Requisitos: Técnicos Cumplimiento de obligaciones legales[28] por parte del Prestador de Servicios

[27] Almark. Ricardo.Obra citada
[28] Ley 25.873 (B.O. 17/12/2003)

Normativa Aplicable. La determinación de la normativa aplicable determina el régimen a aplicar a los servicios. Algunas partes del servicio se rigen por leyes distintas que la que se aplica al contrato: Se debe tener cuidado con la legislación extranjera en cuanto a la protección de datos personales. Se recomienda conocer los distintos tipos de leyes y regulaciones y su impacto potencial en los entornos *cloud.*

4.-Buenas Practicas en la Gestión del Riesgo de la información confidencial o secreta.

Acceso de usuarios con privilegios: El procesamiento de datos sensibles fuera de las instalaciones de la empresa, supuesto del Cloud computing público y comunitario, conlleva un riesgo inherente, conforme el informe de la consultora Gartner[29] es posible que los servicios ofrecidos sorteen los controles físicos, lógicos y humanos por lo que es necesario conocer quien maneja dichos datos, por lo que deberá consensuar con el proveedor para saber quienes son los usuarios con elevados privilegios.

El carácter multi-tenancy de los servicios a través de la nube provoca que varios usuarios estén utilizando los mismos recursos de un modo simultaneo lo que puede dar lugar a que se produzcan accesos no autorizados a la información y que no se segregue la misma adecuadamente. La Soluciones jurídicas serían regular en el contrato las obligaciones del encargado de tratamiento, especialmente la obligatoriedad de compartí-mentalizar la información con el objeto de evitar que se mezcle con la de otros usuarios y como medida de refuerzo la inclusión de las medidas correspondientes en el Documento de Seguridad. Además es aconsejable que se pacte el aislamiento de los datos mediante procedimientos criptográficos pero asegurando la disponibilidad de los mismos-

Sostenemos que siguiendo la Norma IRAM ISO IEC 17.799, se debería identificar la información como un activo y realizar un inventario de los programas, archivo de datos, estructura de datos y soportes de información de acuerdo a la transacción que se lleve a cabo y de los archivos de datos que contenga. Se debe definir al propietario que la necesita para su trabajo y la custodia de acuerdo al área de la organización de que se trate. Ello permitirá su ubicación en una matriz de clasificación que se definió conforme los estándares elegidos, los objetivos de control propuestos y las contramedidas necesarias por tipo y jerarquía de información.

[29] http://www.gartner.com/technology/home.jsp

La autora ha propuesto en su tesis[30] la Definición y confección de una matriz de clasificación, para ello consideró las políticas, estándares, objetivos de control y contramedidas por tipos y jerarquías de las entidades de información de acuerdo con la necesidad y prioridades de las áreas o zonas de la organización con las que se correlacionan y el nivel de confidencialidad necesario para obtener en grado de protección apropiado. Elaboró un cuadro de doble entrada, en el cada entidad o activo de información se representó con filas y los elementos con los que se correlacionan como son: transacción, archivo, soporte, propietario, jerarquías se situaron en las columnas.

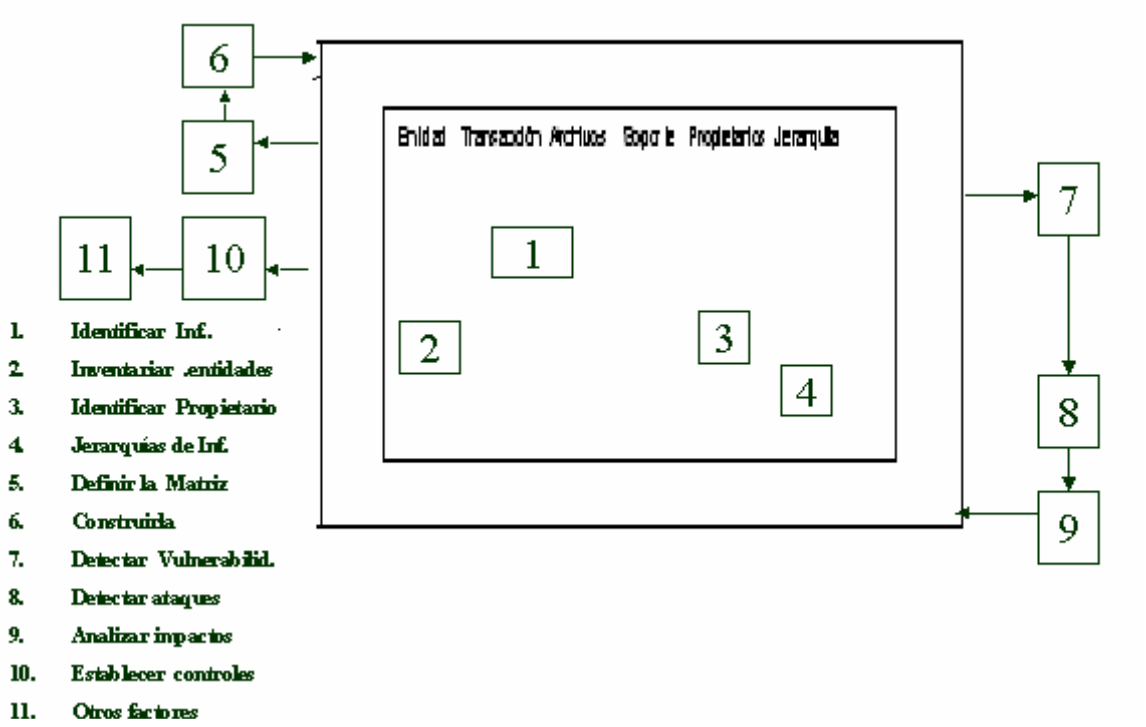

Fig.1: Matriz de Clasificación de la información (Fuente de elaboración propia a partir de datos primarios)

Esta metodología de clasificación de la información ayuda a clasificar las entidades de información de una manera sencilla, al igual que la metodología de Prevención de riesgos

[30] Becerra María del Carmen. Tesis de Informática .Universidad Nacional de la Matanza. Metodologías para la seguridad de la Información del Proceso Penal.

informáticos denominada PRIMA[31] es de tipo cualitativo subjetivo y nos permite utilizar conceptos abiertos que permiten añadir en la herramienta niveles o jerarquías, estándares y objetivos a cumplir en el nivel y ayudas de contramedidas de seguridad.

Cumplimiento normativo:

Los clientes conforme la Ley 25.326[32], son en última instancia los responsables de la seguridad e integridad de sus datos, sin embargo los proveedores de servicios de Internet en nuestro país están sujetos también por las leyes de Telecomunicaciones, a deberes genéricos de confidencialidad en cuanto al almacenamiento y conservación de contenidos[33]. También deben tener en cuanta la Ley 25.520[34] de inteligencia Nacional y la Ley 26.388[35] que penaliza el acceso indebido a los bancos de datos personales

Localización de los datos:

Se debe consultar con los proveedores cual es al marco regulatorio aplicable al almacenamiento y procesamiento de datos, siendo una buena práctica cerrar un acuerdo con el proveedor para que el tratamiento de los datos se subyugue al marco legal del país del suscriptor del servicio.

Aislamiento de datos:

En el cloud las empresas comparten la infraestructura con datos de otros clientes, el proveedor debe garantizar el aislamiento de los datos de los clientes, se recomienda el cifrado, pero el problema son los datos en reposo y tal procedimiento debe ser llevado a cabo por personal especializado dado que un error puede afectar la disponibilidad de los datos.

Recuperación:

El riesgo de recuperación es alto, el acceso a los recursos en la nube depende de la conexión a Internet. Nivel de conexión a la nube del 100% es imposible. La falta de conexión puede dar lugar a la paralización de la empresa. El Incremento de las necesidades de ancho de banda puede dar lugar a un aumento de los costes. Seguridad de

[31] Gonzalez Zubieta, José María. Auditoria Informática. Un enfoque Práctico. Cap3. Metodologías de control interno, seguridad y auditoria informática. Ed. Alfa Omega. 2001.
[32] Ley de Protección de datos personales
[33] http://www.hfernandezdelpech.com.ar/PDF-PubliTrabPrivaAutoEraDigital.pdf
[34] Ley 25.520 (B.O: 06/12/2001)
[35] Ley 25.388 (B.O.25/06/2008)

la Información Perdida de control por el Usuario de la gestión de la seguridad de la información alojada en la nube. Posible acceso por parte de terceros no autorizados. Perdida de datos. Se pueden sufrir/realizar infracciones de la propiedad intelectual por los usuarios.

Soporte investigativo:

La utilización de la nube puede producir una deslocalización de la información y de la custodia de los datos o de la información, pudiendo ser custodiado por diferentes entidades. Sería necesario preparar un procedimiento para gestionar la creación de evidencias electrónicas validas en juicio y un protocolo de actuación que regule la solicitud de las mismas bien por parte de la administración o bien por parte del cliente.

También se aconseja la creación de una base de datos central de conocimiento en el uso de la nube identificando quién custodia los datos, que tipo de datos son, y el uso que se realiza de los mismos. El objetivo es poder tener una idea de la ubicación de los datos para cubrir las necesidades de acceso a los mismos en supuestos de litigios o aportación de los mismos a juicio. Además los contratos de la nube que supongan una creación, uso o almacenamiento de datos en un tercero deberán incluir las siguientes previsiones: Aclarar la propiedad de los datos. Acceso a los datos: quien, cuando, donde y como. Coste para la identificación y búsqueda de la información. Registro de la no Retención de datos: mínimo y máximo de retención, formato. Destrucción y/o procedimiento de devolución de los datos y verificación. Almacenamiento de datos segregación y requisitos de seguridad datos, seguridad. Descubrimiento y/o reunión y concesión de participación. Capacidad de conservación: identificación, ubicación, recuperación, grabación. Auditoría de cumplimiento de los extremos anteriores. Penas por incumplimiento.

Según Gartner la actividad de investigación puede tornarse imposible dado que los datos y los registros de la actividad de múltiples clientes pueden estar juntos o desperdigados por una gran cantidad de equipos y centros de datos. Si bien en nuestro país el usuario está obligado por Ley a realizar copias de seguridad de determinada información al objeto de impedir su perdida, no es menos cierto que en la medida en que dicha información está gestionada a través de la nube el usuario pierde el control sobre la información. Por eso es necesario regular en el contrato, las obligaciones del encargado del Tratamiento a quien le corresponderá la obligación de llevar a cabo las copias de seguridad y la Inclusión de un Documento de seguridad para custodio de los datos.

Viabilidad a largo plazo:

En un entorno ideal un proveedor Cloud permanecerá en el mercado dando un servicio de calidad, pero el mercado es cambiante y cabe la posibilidad que el proveedor sea comprado o absorbido por alguno con mayores recursos.

Posible Incompatibilidad con otros Proveedores

Existe un riesgo muy alto de cautividad respecto del proveedor de servicios esto genera que el usuario posea una fuerte dependencia del proveedor de servicios. Habría que propiciar iniciativas dirigidas a promover una nube abierta que permita a los distintos agentes actuar con plena libertad garantizándose un régimen de libre competencia.

Colisiones con derechos de propiedad intelectual y su seguridad.

La nube puede ser un entorno poco seguro para poner contenidos sujetos a PI de consumo típicamente lineal (películas, música, e-books) a disposición de terceros o retransmitir linealmente (streaming), la captación "pirata" de la transmisión o puesta a disposición de los contenidos, dan lugar a una copia "pirata" que puede ser comercializada. No obstante, es un entorno seguro para ejecutar contenidos sujetos a PI de consumo típicamente interactivo (software, videojuegos) que vayan a ser usados o consumidos interactivamente en la nube de forma que sólo se puedan ejecutar en la nube, sin acceder al archivo que los contiene en el servidor y sin que se puedan copiar ni instalar en el Terminal propio del usuario.

La pérdida de gestión de control de los sistemas de información por parte del Usuario dificulta el conocimiento de aquellas quiebras de seguridad que pudiesen producirse en las infraestructuras del Proveedor. Soluciones jurídicas Regulación por vía contractual de los mecanismos para la notificación de incidencias por parte del Proveedor al Usuario, así como la redacción de un Protocolo para la gestión de las mismas. Inclusión del procedimiento en el Documento de Seguridad del Proveedor.

Aspectos Legales Laborales

En cuanto que la gestión de los sistemas utilizados por los Usuarios, hay que tener en cuenta que se realiza por un tercero y que el cumplimiento del deber de vigilancia de la actividad de los empleados por parte del Usuario se ve limitada. Por otro lado, el Proveedor debe comprobar el adecuado uso de los servicios por parte de los empleados del Usuario. Riesgo de intromisión en los derechos a la intimidad del trabajador. La posibilidad de acceder desde cualquier punto de conexión puede dar lugar al uso fraudulento de la identidad de los usuarios finales y a la extracción de la información y violación de las obligaciones de confidencialidad.

Como soluciones jurídicas se propone la Implantación de un protocolo uso de herramientas informáticas dirigido a los trabajadores en los que se informe: Del uso que deben hacer de las aplicaciones ubicadas en la nube, tanto profesional como privada que dependerá de las características de la aplicación. De la gestión de los nombres de usuario y contraseña. De las consecuencias, sanciones, por un uso inadecuado. De quien va a hacer el seguimiento y control de la actividad en la nube De la obligación de secreto por parte de los Usuarios.

5. Conclusiones:

En el presente trabajo se ha realizado un análisis global de la seguridad y protección de la confidencialidad de archivos digitales, se propone, entre varias recomendaciones, la implementación de normas y procedimientos para la administración segura de la información y se pone énfasis en los aspectos contractuales que se suscitan con las empresas proveedoras de servicios, en la medida que se vayan haciendo más complejos, la diversidad de servicios que ofrece el Cloud, se deberían negociar contratos a medida que se ajusten a los requerimientos de la organización, para asegurar la minimización del riesgo.

También se sugiere que cualquiera sea la infraestructura cloud que se contrate (redes, serviciares, aplicaciones, almacenamiento y otro) se deben identificar los riesgos y valorarlos poniendo énfasis en:

La **seguridad y la propiedad de los datos** es uno de los aspectos clave. Los informes muestran una gran preocupación por la propiedad y el tratamiento de los datos dado que estas infraestructuras pueden gestionar los datos en múltiples países lo que puede generar conflictos en cuanto al marco legal en el que son tratados. También se plantea que estos entornos, al manejar gran cantidad de datos, pueden ser objeto de fugas de información, ya sean intencionadas o fortuitas.

El **cumplimiento normativo en entornos *cloud.*** En este caso el problema se presenta debido a la falta de transparencia de estas infraestructuras, y sobre todo de cómo se han implantado, las organizaciones ceden el control directo de muchos aspectos de la seguridad por lo que otorgan un nivel de confianza sin precedentes al proveedor del servicio. El suscriptor ignora como y donde son almacenados sus datos, o como se protegen, por lo que es muy recomendable que el suscriptor del servicio se informe claramente de cómo se gestiona el entorno. Para la creación de un servicio *cloud* interviene multitud de software de distintos proveedores. Es decir, son **entornos complejos** por lo que se ha de poner especial atención a las posibles vulnerabilidades del mismo e implantar procedimientos de parcheado.

La **identidad y el control de acceso**. Es otro aspecto a considerar como importantes Por lo general, la mayoría de las infraestructuras son compartidas por múltiples empresas o

usuarios y la mala definición de los controles de acceso puede provocar accesos no autorizados a datos confidenciales. La definición de una buena política de identidad y control de acceso basada en políticas de mínimo privilegio es esencial en entornos *cloud*.

Contratos de acuerdo de servicio, Todas las recomendaciones en cuanto a este asunto indican que éstos deben de ser revisados y creados específicamente, detallando los controles, las normativas, las medidas de protección, los plazos de recuperación del servicio. Además hay que tener en cuenta que por tratarse de servicios complejos las garantías de responsabilidad y rendimiento pueden convertirse en una problema serio.

Estructura Organizacional: Cualquiera sea la actividad o ramo de la organización, estas deben adecuar su estructura orgánica-funcional y guardar analogía con la usado en el cloud para la implementación, seguimiento y control de las políticas de seguridad y la administración de los procedimientos y los estándares para la administración segura de la información. Además se deben establecer mecanismos de auditoria y herramientas para que se sigan las políticas de la organización durante el ciclo de vida.

Referencias Bibliográficas:

1. Brenna Ramón Gerónimo. Internet y la Privacidad. Reflexiones sobre la sociedad de la información y la recolección de datos on line. Depalma. 2002.

2. Almark, Daniel Ricardo. El contrato de Outsourcing de Sistemas de Información. Bs.As. Lexis Nexis. Argentina 2006

3. Gonzalez Zubieta, José María. Auditoría Informática. Un enfoque Práctico. Cap Metodologías de control interno, seguridad y auditoria informática. Ed.Alfa Omega.2001.

4. IRAM (Instituto Argentino de Normalización)."Esquema de normativa IRAM ISO IEC 17.799. 2002.

5. CSA, 2010, Top Threats to Cloud Computing V1.0

6. Gartner, 2008, Assessing the Security Risks of Cloud Computing

7. NIST, 2011, Guidelines on Security and Privacy in Public Cloud Computing

Sitios Web consultados:

www.isaca.org.CISA

www.arcert.gov.ar/PSI_Modelo