INFOTEC CENTRO DE INVESTIGACIÓN E INNOVACIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

DIRECCIÓN ADJUNTA DE INNOVACIÓN Y CONOCIMIENTO

GERENCIA DE CAPITAL HUMANO

Posgrados

"PROPUESTA DE IMPLEMENTACIÓN DEL USO DE LA NUBE POR EL DEPARTAMENTO JURÍDICO DE EMPRESA PARA LA CONTRATACIÓN DE PERSONAL"

SOLUCIÓN ESTRATÉGICA EMPRESARIAL

Que para obtener el grado de MAESTRO EN DERECHO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

Presenta:

Stephanie Michelle Avalos García

Asesor:

Dr. Alberto Nava Garcés

Ciudad de México, 31 de octubre de 2017.

Autorización de impresión

C4

AUTORIZACIÓN DE IMPRESIÓN

Ciudad de México, 31 de octubre de 2017

La Gerencia de Capital Humano/ Gerencia de Investigación hacen constar que el proyecto terminal titulado:

"Propuesta de implementación del uso de la nube por el departamento jurídico de empresa para la contratación de personal"

Desarrollada por el alumno

Nombre: **Stephanie Michelle**

Apellido paterno: **Ávalos**

Apellido materno: **García**

Desarrollado bajo la asesoría del:

Dr. Alberto Nava Garcés

Ha sido revisada y aprobada por el profesor investigador:

Mtra. Evelyn Téllez Carvajal

Quien ha sido depositado a esta Gerencia en su oportunidad sus reflexiones y comentarios que han sido atendidos e integrados en su totalidad por el alumno a la nueva versión escrita del proyecto integrado revisado; siendo corroborados por los mismos revisores, quienes emitieron sus votos aprobatorios por separado que obran en el expediente de investigación correspondiente.

Por lo cual, se expide la presente autorización para impresión del proyecto terminal al que se ha hecho mención.

Vo. Bo.

Mtra. Patricia Ávila Muñoz
Gerencia de Capital Humano

*Anexar a la presente autorización al inicio de la versión impresa del proyecto integrado que ampara la misma.

Tabla de contenido

Introducción 1

Capítulo 1. La protección de datos personales en México 4

1.1 Antecedentes y conceptos 4

1.2 Marco jurídico 6

1.3 Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) 8

1.4 Principios y deberes durante el tratamiento de datos personales 11

1.5 Los datos personales en el cómputo en la nube 14

Capítulo 2. Cómputo en la nube 17

2.1 Definición 18

2.2 Tipos de nube 19

2.2.1 Nube pública 19

2.2.2 Nube privada 21

2.2.3 Nube híbrida o mixta 22

2.3 Ventajas del uso de la nube 23

2.4 Desventajas del uso de la nube 25

Capítulo 3. Propuesta de implementación del uso de la nube por el departamento jurídico de empresa para la contratación de personal 30

3.1 Propuesta de modelo de implementación de nube 31

3.2 Medidas de seguridad 35

3.3 Riesgo por el tipo de dato 36

3.4 Propuesta de implementación de nube en proceso de contratación de personal 37

3.4.1 Búsqueda de candidatos 37

3.4.2 Entrevistas 39

3.4.3 Exámenes 39

3.4.4 Creación de expediente 41

3.4.5 Análisis de riesgo por el tipo de dato 43

3.4.6 Medidas de seguridad recomendadas 44

Conclusiones 49

Bibliografía 51

Artículos de revista 52

Anexos 54

Anexo I 54

Anexo II 55

Anexo III 56

Índice de figuras

Figura 1. Conceptos tratamiento, uso, remisión y transferencia 9

Figura 2. Interrelación de sujetos 10

Figura 3. Servicios legales en empresa 31

Figura 4. Propuesta adaptada del modelo de tres fases 32

Índice de cuadros

Cuadro 1. Análisis de riesgo 44

Introducción

Los avances tecnológicos pueden convertirse en herramientas que aseguren el cumplimiento de las disposiciones legales tal es el caso del uso de la nube para asegurar el adecuado tratamiento de los datos personales.

Sin embargo, en la mayoría de empresas, desde pequeñas hasta grandes, los abogados no tienen confianza de resguardar la información en un servidor común (nube) a pesar de los múltiples beneficios que se obtienen, tales como la disminución de pérdidas de información por fallas en equipos, la administración más eficiente de la documentación, una mejor supervisión, etc.[1]. Esto es debido, en la mayoría de ocasiones, a la falta de conocimiento en el tema, ya que no existe información dirigida a la práctica legal en empresa que explique el uso de la nube como herramienta para mejorar los procesos y así disminuir las contingencias legales.

Considerando lo anterior y a efecto de dar cumplimiento a las disposiciones en materia de datos personales, presento la propuesta de tratamiento de datos personales en la implementación de la nube en un departamento jurídico respecto al proceso de contratación de personal.

Decidí abordar la contratación de personal, toda vez que cualquier organización, sin importar el tamaño o tipo de actividades, requiere recursos humanos para operar lo que implica el tratamiento de datos personales con alto nivel de riesgo por involucrar datos personales patrimoniales y sensibles, que pueden generar cuantiosas contingencias legales en caso de no llevar un manejo adecuado.

La propuesta se integra por tres capítulos. Los dos primeros capítulos consisten en una breve descripción de la normativa aplicable a datos personales en posesión de particulares y explicación de los tipos de nube. En el tercer capítulo se describe la operación general del departamento jurídico de cualquier empresa y se

[1] Joyanes, Luis, Computación en la nube. Estrategias de Cloud Computing en las Empresas, México, Alfa omega, 2012, p. 27.

propone un plan de implementación de la nube con un enfoque a la protección de datos personales en la contratación de personal.

La propuesta de estrategia se desarrolló con base en el método empírico-analítico en virtud que se consideró la operación diaria de la contratación de personal en lo general, sin incluir excepciones a los filtros de selección de personal ni considerando personal especializado.

Respecto a la diagramación de procesos, se utilizó la metodología *Rummler y Brache*, la cual consiste en el análisis del flujo de trabajo en tres niveles: empresa, procesos y tareas (o trabajo) para identificar la interacción entre los sujetos involucrados y las actividades que desempeñan, orientándolos a los objetivos de la organización. La diagramación de los procesos se integró por dos etapas: el mapeo *"as is"* es decir, como se opera al momento del levantamiento, y el mapeo *"to be"* que incluye las mejoras en el flujo de conformidad a los objetivos que pudieran ser de interés para cualquier empresa: eficiencia durante el proceso sin afectar la seguridad jurídica.

Finalmente, para realizar una adecuada implementación de procesos que involucran datos personales es necesario realizar un levantamiento de los datos personales involucrados y el nivel de riesgo de los mismos, por lo que se eligió la metodología de análisis de riesgo BAA, la cual ha sido desarrollada por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) como guía en la autodeterminación vinculante de los responsables. La metodología BAA se integra por valores predeterminados para identificar el riesgo latente y las medidas de seguridad aplicables para el riesgo de que se trate. El riesgo latente se determina considerando el beneficio para el atacante, la posibilidad de accesos y la anonimidad durante la vulneración de la información. En los tres casos, el INAI ha establecido valores considerando tipo de dato, volumen de titulares, cantidad de accesos y entorno en el que se encuentran los datos personales.

Capítulo 1

La protección de datos personales en México

Capítulo 1. La protección de datos personales en México

La protección de los datos personales es de reciente inclusión en el sistema jurídico mexicano, por lo que a pesar de estar presente el tratamiento en todas las actividades económicas en el país, son pocos los abogados que estudian la regulación para proponer estrategias de protección, por lo que es recomendable conocer los antecedentes para comprender la evolución y concientizar en la importancia de la protección de los datos personales.

1.1 Antecedentes y conceptos

La protección de datos personales forma parte del Derecho a la Intimidad o el Derecho a la Privacidad según el sistema de derecho aplicable, siendo continental europeo o anglosajón, respectivamente[2].

El Derecho a la Intimidad tiene su antecedente formal más antiguo en la legislación francesa, artículo 11 de la Ley de Mayo de 1868 relativa a la prensa, que sanciona cualquier publicación relativa a la vida privada con una multa de 500 francos[3]. Veintidós años después, el Derecho a la Privacidad se conceptualiza en el ensayo *The Right to Privacy* publicado 1890 por Samuel Warren y Luis Brandeis, en el cual se establece la evolución de la protección *common law,* destacando el derecho a "no ser molestado" (*right to be let alone*)[4] y que se complementa en los años sesenta con la propuesta de Alan Westin, consistente en el derecho del individuo para determinar los alcances en que su información personal será comunicada a los demás[5].

De lo anterior se desprende que el Derecho a la Intimidad (y a la Privacidad) se integra por el derecho a aislarse de los demás (derecho a no ser molestado) y el

---

[2] Celis, Marcos, "La Protección de la Intimidad como Derecho Fundamental de los mexicanos", *Estudios en Homenaje a Marcia Muñoz de Alba Medrano*, México, UNAM, 2006, pp. 71-106.
[3] *Loi Relative a la Presse. 11 Mai 1868. "11. Toute publication dans un écrit periodique relative à un fait de la vie privé constitue une contravention punie d'un amende de cinq cent francs."*. Ibídem p. 75.
[4] Warren, Samuel y Brandeis, Louis, "The Right to Privacy", *Harvard Law Review*, Estados Unidos de América, Vol. IV, No. 5, diciembre 1890.
[5] García, Diego, "Derecho a la Privacidad", *Derechos Humanos en la Constitución: Comentarios de Jurisprudencia Constitucional e Interamericana,* México, Suprema Corte de Justicia de la Nación, 2013, pp. 1045-1075.

derecho a controlar la información relativa a uno mismo (derecho a la autodeterminación informativa), siendo este último aquel al que le corresponde proteger los datos personales.

Los datos personales o información nominativa, según Marcia Muñoz de Alba es "aquella información que permite revelar la identidad de una persona física"[6]. De esto se deduce que el dato personal no tendrá restricción respecto a la longitud, cantidad, naturaleza ni al soporte material que lo contenga, por lo que los datos personales podrán consistir en garabatos, números, imágenes y sonidos, sin importar que se encuentren en el plano físico o digital. La única característica que deberá cumplir cualquier información para considerarse dato personal, deberá ser que se asocie con la identidad de alguna persona física.

Por lo que hace a las personas morales, tanto la ley como la doctrina no estiman que sean titulares de datos personales, toda vez que la intimidad es un concepto relacionado únicamente a personas físicas, lo cual se aclara en 2014, cuando la Suprema Corte de Justicia de la Nación estableció la tesis aislada "Personas morales. Tienen derecho a la protección de los datos que puedan equipararse a los personales, aun cuando dicha información haya sido entregada a una autoridad", que "los bienes protegidos por el Derecho a la Privacidad y de protección de datos de las personas morales, comprenden aquellos documentos e información que les son inherentes, que deben permanecer ajenos al conocimiento de terceros…", e incluso confirma el criterio, cuando en líneas siguientes obliga a las autoridades que reciban datos de personas morales, a mantener la confidencialidad de aquellos datos que sean similares a los personales "…la información entregada a las autoridades por parte de las personas morales, será confidencial cuando tenga el carácter de privada por contener datos que pudieran equipararse a los personales…"[7]. Del texto de la tesis se interpreta que, aunque las personas morales no son titulares de datos personales, la información que sea similar a éstos, tendrá un nivel de confidencialidad al otorgado a personas físicas.

---

[6] Muñoz de Alba, Marcia, "Habeas Data", *Estudios en Homenaje a Marcia Muñoz de Alba Medrano*, México, UNAM, 2006, p. 3.
[7]Tesis aislada 2005522. P. II/2014, *Semanario Judicial de la Federación y su Gaceta,* Décima Época, libro 3, febrero de 2014, p. 274.

Existen datos personales que por su naturaleza requieren un mayor nivel de protección: los datos financieros o patrimoniales y los datos personales sensibles, entendiéndose los últimos como aquellos que corresponden al espacio más privado del individuo o aquellos cuya divulgación pueda menoscabar las libertades del titular por su potencial para generar actos de discriminación o exposición a riesgos graves. Ejemplos de datos sensibles son las preferencias sexuales, creencias religiosas, ideología política, etc. El acceso no autorizado de datos personales sensibles, solo estará justificado por el impacto social que se pueda generar y bajo supuestos previamente determinados en la legislación aplicable.

Por lo que hace al Derecho Procesal o Adjetivo de la protección de datos personales, se cuenta con el *habeas data*, que según Muñoz de Alba, es el "recurso procesal diseñado para controlar la información personal contenida en bancos de datos, cuyo derecho implica la corrección, la cancelación, y la posibilidad de restringir y limitar la circulación de los mismos"[8]. El *habeas data* se clasifica según su finalidad en "propio", cuando está dirigido a prevenir y reparar daños por el uso de datos personales, y en "impropio" cuando también tiene como objetivo garantizar el acceso a la información de autoridades[9].

El *habeas data* se integra por dos fases para proteger los datos personales. La primera consiste en el ejercicio de los derechos de acceso, rectificación, cancelación y oposición (ARCO) del titular ante el responsable del tratamiento de sus datos personales, para lo cual, el último deberá señalar el procedimiento para que el titular pueda ejercer sus derechos en el Aviso de Privacidad. La segunda fase surge cuando el titular estima que el responsable no le permitió ejercer sus derechos, y se lleva a cabo ante la autoridad que señale la legislación correspondiente.

1.2 Marco jurídico

En México el Derecho a la Intimidad ha tenido presencia en la Constitución actual desde su promulgación en 1917 con el "derecho a no ser molestado" que está

[8] Muñoz de Alba, Marcia, *op. cit.*, nota 6. p.3.
[9] Puccinelli, Oscar, "Evolución histórica y análisis de las diversas especies, subespecies, tipos y subtipos de habeas data en América Latina. Un intento clasificador con fines didácticos", *Vniversitas*, Colombia, número 107, 2004.

consagrado en el artículo 16 con la inviolabilidad de comunicaciones y el derecho a no ser molestado salvo por mandato escrito de autoridad que esté fundado y motivado.

Por otra parte, el "derecho a la autodeterminación informativa" aparece en abril de 2009, cuando se faculta al Congreso a legislar en materia de datos personales en posesión de particulares y en junio 2009 se publican las modificaciones constitucionales que reconocen el derecho a la protección de datos personales (artículo 16 segundo párrafo) y el *habeas data* para datos personales y acceso a la información pública.

Los aspectos relevantes derivados de la reforma constitucional para la protección de datos personales son:

- Reconocimiento del derecho a la protección de datos personales.
- Se faculta al titular de los datos personales a acceder y/o rectificarlos sin necesidad de acreditar interés ni justificación.
- Creación del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI antes IFAI) como organismo autónomo, especializado, imparcial, colegiado, con personalidad jurídica y patrimonio propio para vigilar el cumplimiento de las disposiciones en materia de privacidad a nivel federal.
- Establece que será de jurisdicción federal la regulación y vigilancia de datos personales en posesión de particulares, sujetos obligados y autoridades de orden federal.
- Define como sujeto obligado a todos aquellos que lleven a cabo actos de autoridad y/o reciban recursos públicos, incluyendo así a sindicatos, fideicomisos públicos, partidos políticos, órganos autónomos y concesionarios.
- A nivel federal existen dos ordenamientos encargados de vigilar el cumplimiento a la protección de datos personales según el sujeto que tenga la posesión de los datos personales de terceros: Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) publicada en julio 2010, y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LDPPSO) publicada en enero 2017.

Las legislaciones locales deberán emitir los ordenamientos aplicables a Sujetos Obligados de cada Entidad Federativa en el entendido que deberán alinearse a las disposiciones federales.

1.3 Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP)

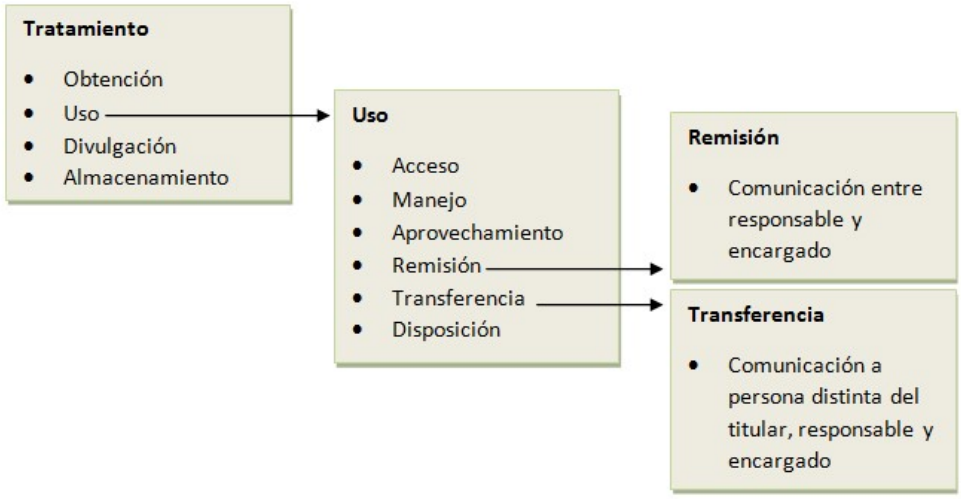
La LFPDPPP es el instrumento jurídico en el que se establecen los conceptos, principios, derechos de los titulares, regulación para la transferencia de datos, autoridades, procedimientos para la protección de derechos, sanciones y delitos, de todos aquellos datos que estén en posesión de particulares, por lo que aplica a todas las personas de carácter privado siempre que no sean sujetos obligados según definición constitucional, sociedades de información crediticia y personas que almacenen datos para uso personal, sin fines comerciales y de divulgación.

El Reglamento de la LFPDPPP prevé que no se aplicará lo dispuesto en referido ordenamiento a los datos de las personas morales, datos personales de personas físicas en su calidad de comerciantes y profesionistas con relación al producto/ servicio que provean a quien recibe los datos, datos almacenados en agendas personales, datos personales cuyo acceso implique plazos o actividades desproporcionadas, e información básica de empleados (nombre, funciones, puestos desempeñados, domicilio y datos de contacto).

Existen términos que en el lenguaje común podrían parecer sinónimos, sin embargo para efectos de la LFPDPPP se deberá distinguir de manera clara cada concepto a efecto de cumplir con las disposiciones relacionadas, tales como los conceptos derivados del tratamiento de los datos y los sujetos en contacto con los datos personales.

El tratamiento de datos se integra por la obtención, el uso, la divulgación y el almacenamiento. El uso es el acceso, manejo, aprovechamiento, transferencia y disposición de los datos. La transferencia consiste en el envío de datos a una persona distinta del titular, responsable y encargado de los datos. La remisión es el intercambio de información entre el responsable y el encargado.

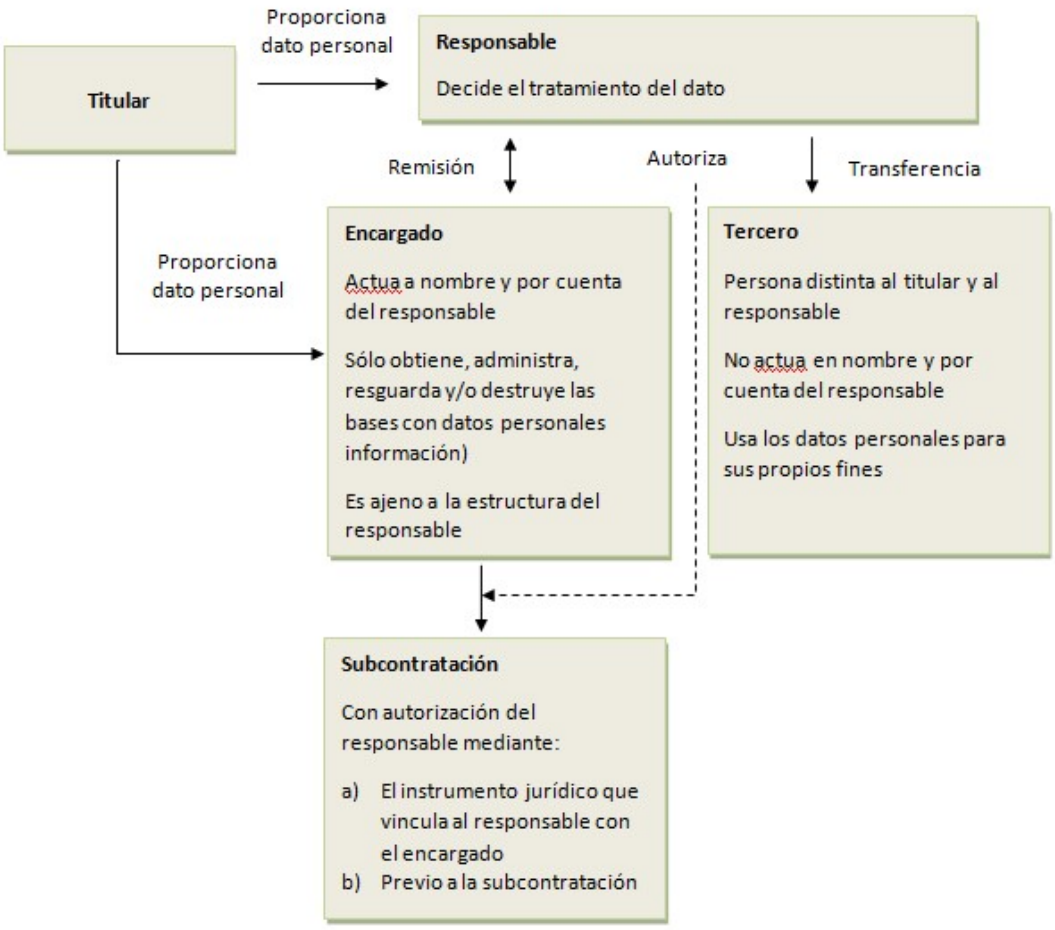
Figura 1. Conceptos tratamiento, uso, remisión y transferencia



Fuente: Elaboración propia de acuerdo a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares

En cuanto a los sujetos, la LFPDPPP considera a los siguientes: “titular” del dato personal; “responsable” quien es la persona que decide el tratamiento de los datos; “encargado” quien trata los datos por cuenta del responsable y, el “tercero” quien no es ni el titular ni el responsable. El encargado podrá subcontratar servicios que lleven a cabo tratamiento de los datos personales siempre que dicha subcontratación cuente con autorización del responsable.

Figura 2. Interrelación de sujetos



Fuente: Elaboración propia de acuerdo a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares

Los avances tecnológicos y el incremento de operaciones internacionales facilitan el tratamiento de datos personales fuera de territorio nacional, siendo aplicable la LFPDPPP cuando el responsable esté ubicado en territorio mexicano (aunque el encargado esté en el extranjero). Si el responsable está ubicado en el extranjero, le será aplicable la legislación mexicana cuando así lo acuerde por contrato o lo determine el derecho internacional o que si utiliza medios situados en el país para el tratamiento de los datos (exceptuando actividades de tránsito de datos sin tratamiento).

En caso que el responsable no se encuentre ubicado en territorio mexicano, pero el encargado sí tenga establecimiento en México, a este último le serán aplicables además de las obligaciones propias como encargado, aquellas relativas a las medidas de seguridad.

1.4 Principios y deberes durante el tratamiento de datos personales

Con la finalidad de garantizar la protección de los datos personales, La LFPDPPP considera ocho principios y dos deberes que deberá cumplir todo aquel que tenga posesión de datos personales[10], teniendo como límite la afectación de derechos de terceros y la protección de la seguridad nacional, el orden, la seguridad y la salud públicos.

Principio de licitud. Los datos personales deberán tratarse con apego a lo señalado en la normativa aplicable, es decir, el responsable solo podrá hacer aquello que esté legalmente permitido. La normativa aplicable, además de la LFPDPPP, será toda aquella que corresponda al caso concreto, pudiendo abarcar los sectores financieros y de salud, así como legislación internacional que esté relacionada por la territorialidad del tratamiento de los datos y/o en alcance a Tratados Internacionales en materia de Derechos Humanos.

Principio de lealtad. No se podrán recabar los datos con dolo, mala fe o negligencia, toda vez que la entrega de datos personales se lleva a cabo con la confianza de que solo se utilizarán para los fines señalados por quien los recibe.

Principio del consentimiento. Todo tratamiento de datos deberá contar con el consentimiento del titular, excepto cuando los datos figuren en fuentes de acceso público, los datos sean disociados, tengan como propósito cumplir con obligaciones entre el titular y el responsable, por causas de emergencia que puedan dañar al titular y/o sus bienes, emergencias médicas si el titular no está en condiciones de otorgar el consentimiento y quienes realicen el tratamiento de datos esté sujeto a secreto profesional, por mandato de ley y por resolución de autoridad competente.

[10] INAI, *Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares,* México, INAI, julio 2016.

El consentimiento deberá ser otorgado para finalidades específicas; podrá ser tácito, expreso y expreso por escrito según el tipo de dato personal de que se trate. El consentimiento tácito se obtiene cuando el Titular no se opone al tratamiento de los datos cuando se puso a su disposición el aviso de privacidad. El consentimiento expreso implica una acción "de autorización" por parte del Titular para el tratamiento de los datos personales y aplica para datos patrimoniales y financieros. El consentimiento expreso y por escrito es requisito indispensable para el tratamiento de datos personales sensibles y deberá contar con huella digital o firma del titular.

Principio de información. A través del aviso de privacidad, el responsable deberá informar al titular la información que se recabará y con qué fines. En caso de ser necesario, el responsable tendrá que generar los avisos de privacidad que requiera según la operación relacionada a datos personales. El aviso de privacidad deberá ser sencillo, con información necesaria, de estructura y diseño de fácil entendimiento, lenguaje claro y comprensible. El medio por el cual se comunicará el aviso deberá ser acorde a la forma en que se obtienen los datos personales. Existen tres modalidades de aviso de privacidad y será aplicable según las características en que se recaban los datos personales, siendo el aviso de privacidad "corto" cuando el espacio es limitado y los datos recabados son mínimos; el aviso de privacidad "simplificado" cuando los datos se obtienen de manera directa del titular; y el aviso de privacidad "integral" cuando se obtienen los datos de manera personal. Cabe señalar que los avisos de privacidad corto y simplificado deberán prever los mecanismos por los cuales el titular podrá consultar el aviso de privacidad integral. Se exceptuará la obligación del principio de información cuando los datos se obtengan de manera indirecta y sean para fines históricos, estadísticos o científicos.

Principio de proporcionalidad. Los datos personales que se recaben deberán ser sólo aquellos que sean necesarios para la finalidad con la que fueron recabados, es decir, sólo aquellos que sean necesarios, adecuados y relevantes. Para el caso de datos personales sensibles, su conservación deberá limitarse al periodo mínimo necesario y no se podrán realizar bases de datos salvo que sea mandato legal, se

justifique para temas de seguridad nacional, orden, seguridad y salud públicos, o el responsable lo requiera para finalidades legítimas acordes con los fines de la obtención de los datos.

Principio de finalidad. Los datos recabados solo podrán ser tratados para cumplir con la finalidad señalada en el aviso de privacidad, la cual deberá ser clara y determinada, evitando expresiones ambiguas. Los avisos de privacidad podrán identificar finalidades primarias, que son indispensables para la relación entre el titular y el responsable, y las finalidades secundarias, respecto de las cuales el titular podrá negar o revocar su consentimiento, sin afectar el tratamiento de las finalidades primarias. El responsable deberá prever en el aviso de privacidad el mecanismo para oponerse o revocar su consentimiento para finalidades secundarias. No se podrá condicionar el cumplimiento de las finalidades primarias a la aceptación de las finalidades secundarias.

Principio de calidad. Los datos personales que se recaben deberán ser exactos, completos, pertinentes (que efectivamente corresponden al titular), correctos y actualizados. En caso que los datos se obtengan directamente del titular, se presumirá que cumplen con este principio hasta que el propio titular manifieste lo contrario o el responsable tenga prueba en contrario. Los datos obtenidos de manera indirecta deberán contar con medidas razonables para cumplir con el principio de calidad.

Los datos personales deberán conservarse solo por el tiempo necesario para cumplir con las finalidades agregando los plazos legales, administrativos y fiscales que correspondan, así como el periodo de bloqueo, que consiste en el plazo que deberán conservarse los datos para su acceso en caso que sea necesario determinar responsabilidades de su tratamiento. Es de destacar que la LFPDPPP contiene disposición expresa para eliminar cualquier información relacionada al incumplimiento de obligaciones contractuales una vez que transcurran seis años a partir del incumplimiento. Los procedimientos de conservación, bloqueo y supresión de datos personales deberán documentarse por el responsable.

Principio de Responsabilidad. Es el principio de rendición de cuentas por el cual el responsable se obliga a la observancia de todos los principios y deberes,

incluso cuando los datos personales sean tratados por encargados. El responsable deberá tomar las medidas necesarias para que el aviso de privacidad cumpla con los requisitos que señala la normativa y facilitar que el titular ejerza los derechos relativos a sus datos personales.

Deber de Confidencialidad. Es la obligación a cargo del responsable de mantener la secrecía de los datos personales durante y después del tratamiento de los datos personales.

Deber de Seguridad. Es la obligación de establecer medidas de seguridad para proteger los datos personales de daños, pérdidas, alteraciones, destrucción, acceso o tratamiento no autorizado. Las medidas de seguridad empleadas para los datos personales deberán ser al menos iguales a las que tenga el responsable respecto a su propia información. Para determinar las medidas de seguridad a implementar se deberá considerar el riesgo por el tipo de dato, las consecuencias en caso que sean vulneradas las bases de datos, sensibilidad de los datos y el desarrollo tecnológico disponible. Una estrategia de seguridad efectiva requiere que se lleven a cabo las acciones señaladas en el artículo 61 del Reglamento de la LFPDPPP. En caso que suceda alguna vulneración a los sistemas de seguridad de los datos personales y está pueda dañar de manera significativa el patrimonio del titular, el Responsable deberá informarle la naturaleza de la vulneración, los datos personales comprometidos, recomendaciones al titular para proteger sus intereses, las acciones correctivas realizadas y los medios de contacto para obtener más información.

1.5 Los datos personales en el cómputo en la nube

La LFPDPPP y su reglamento, atendiendo a las necesidades actuales en el manejo de la información en soportes electrónicos, prevén disposiciones específicas para la contratación de servicios de cómputo en la nube.

Solo se podrá contratar servicios en la nube cuando el proveedor cumpla con los siguientes requisitos:

1. Contar con políticas de protección de datos personales acordes a la legislación nacional.
2. Transparentar subcontrataciones relacionadas a los datos que resguardará.

3. No podrá incluir condiciones que le otorguen titularidad respecto a los datos personales.
4. Guardar confidencialidad de los datos personales a su resguardo.
5. Tener mecanismos para dar a conocer cambios en las políticas de privacidad y condiciones del servicio, y permitir que el responsable limite el tratamiento de los datos personales que resguarda el proveedor del cómputo en la nube.

Capítulo 2

Cómputo en la nube

Capítulo 2. Cómputo en la nube

La ejecución de aplicaciones y el almacenaje de información digital se pueden realizar de manera aislada en un equipo de cómputo o a través de servidores que permiten la ejecución y acceso a través de varios equipos de cómputo. Esta última modalidad de operación es conocida como “cómputo en la nube” o simplemente “nube”.

La implementación de la nube se ha convertido en la prioridad de las entidades públicas y privadas, siendo parte de las agendas digitales de los gobiernos Estatales y sujetos supranacionales, tales como la Unión Europea[11] y la Comunidad Andina[12], toda vez que se ha incrementado exponencialmente su uso en las operaciones cotidianas de las empresas, generando un valor estimado de $47,400 millones de dólares con una tasa de crecimiento anual de 23.5%[13].

En México la reciente reforma de telecomunicaciones presupone un incentivo adicional para la migración a la nube, al permitir mayor acceso a menor costo con una mejor calidad en el servicio de internet por parte de los proveedores de servicios de telecomunicaciones.

El Instituto Mexicano para la Competitividad, A.C. publicó en mayo 2012, un estudio encargado por *Microsoft* para determinar la estimación de ahorros económicos por la adopción de la nube en todas las operaciones privadas y públicas de México, demostrando que la cifra de ahorro equivale al 0.31% del PIB nacional, siendo un 0.23% el ahorro en el sector privado y 0.08% en el sector público, el cual es superior al 0.05% del ahorro estimado del gobierno norteamericano.

Los proveedores de servicios en la nube señalan que existen múltiples beneficios, sin embargo su adopción ha sido lenta y desconfiada por parte del sector público y privado, ya que se trata de una nueva figura de operación que presupone un reto para la normatividad actual.

---

[11] La Unión Europea a través de la Comisión Europea en conjunto con la iniciativa privada, crearon en 2012 la Asociación Europea de Computación en Nube con la finalidad de incrementar el uso de la Nube con requisitos mínimos de seguridad.

[12] Bolivia presentará una iniciativa de ley para otorgar “soberanía” a la nube como parte de un programa piloto de la Comunidad Andina.

[13] Estimación de la empresa IDC (International Data Corporation) en reporte anual 2013.

2.1 Definición

La primera definición oficial de cómputo en la nube la lleva a cabo el Instituto Nacional de Estándares y Tecnología de Estados Unidos de América (NIST)[14] en la publicación especial 800-145[15], definiéndolo como "un modelo que permite el acceso a la red bajo demanda de manera adecuada desde cualquier ubicación, para compartir una serie de recursos de cómputo (ej. Redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser rápidamente proveídos y entregados con un mínimo esfuerzo de administración o interacción en la provisión del servicio".

En México aparece por primera vez la definición de cómputo en la nube, en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada en enero de dos mil diecisiete, en el artículo 3 numeral VI: "Cómputo en la nube: Modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos virtuales, en recursos compartidos dinámicamente".

De las definiciones antes descritas, se desprenden cinco características del cómputo en la nube:

a) Auto-servicio bajo demanda. El usuario solicita la información/ recurso sin necesidad de algún intermediario humano.
b) Amplio acceso a la red. Posibilidad material de conectarse a una red de información desde cualquier dispositivo. Este requisito se cumple aunque el administrador de la red condicione el acceso mediante el uso de diversos medios adicionales de autenticación. La posibilidad tecnológica de acceder subsiste aunque sea controlada por el administrador.

[14] *National Institute of Standars and Technology* pertenece al Departamento de Comercio de Estados Unidos de América, y es responsable de las normas oficiales en campos como la nanotecnología, biotecnología, tecnologías de la información y fabricación avanzada.
[15] Mell Peter, et al. "The NIST Definition of Cloud Computing", *NIST Special Publication*, Estados Unidos de América, número 800-145, septiembre 2011.

c) Conjunto de recursos. El administrador tiene la posibilidad de proveer diversos recursos (almacenamiento, procesamiento, ancho de banda, aplicaciones, etc.) dependiendo las necesidades del usuario.
d) Elasticidad inmediata. Los recursos a los que tendrá acceso el usuario pueden ser ilimitados, en cualquier cantidad y en cualquier momento, de manera inmediata.
e) Medición del servicio. Es posible medir/ monitorear accesos, descargas, almacenamiento, y en general, cualquier dato cuantitativo relacionado a la nube.

Es de destacar que estas características siempre existen en el cómputo de la nube, pero pueden ser controladas por el proveedor del servicio, teniendo facultades de limitar o restringir su uso al usuario final, por ejemplo, la limitación del acceso a ciertos horarios, proporcionar solo el servicio de almacenamiento, etc.

Como consecuencia de lo anterior se desprende que “la nube” es el vehículo (red) que provee los servicios, y el cómputo en la nube es un modelo de acceso a recursos, una estructura compleja que integra diversos recursos materiales físicos y virtuales.

2.2 Tipos de nube

Según la NIST, existen cuatro formas posibles para desplegar la infraestructura del cómputo en la nube: pública, privada e híbrida o mixta y comunitaria, siendo la última de carácter teórico ya que los proveedores solo ofrecen las tres primeras.

2.2.1 Nube pública

Se trata de la nube cuya infraestructura está disponible para el público en general. Puede ser administrada, operada y/o estar en posesión por organizaciones gubernamentales, de negocios y académicas. Se trata de un modelo estándar o generalizado, es decir, no es un sistema hecho a la medida, es un modelo mediante el cual un proveedor de servicios hace disponibles sus recursos mediante una red abierta de telecomunicación (internet).

Para poder prestar los servicios, el proveedor los gestiona mediante su centro de procesamiento de datos (CPD) o *data center*, el cual consiste en el lugar físico que contiene todo el *hardware* en el cual se almacena, procesa y se conecta a la

red, la información y/o procesos necesarios para proveer los servicios de cómputo. Tener un CPD implica un gran costo de inversión en virtud que se integra de equipo especializado de cómputo, tales como servidores, *mainframes, ups, pdu, routers, switches*, discos duros, etc.; alimentación eléctrica, sistemas de enfriamiento, iluminación, entre otros. Así mismo, el consumo de energía es muy alto, por lo que se deberá de cumplir con los lineamientos que estime pertinentes cada Estado a efecto de disminuir el impacto ambiental. La Unión Europea ha sido la primera autoridad que emitió un código de conducta para mejorar la eficiencia energética, que es de carácter potestativo, y el cual ha tenido amplia aceptación por tener estrategias efectivas para disminuir los costos en el consumo de energía.[16]

Cualquier tipo de nube requiere de un CPD, y en el caso de la nube pública, es el proveedor de servicios quien absorbe todo el costo de la infraestructura para proporcionar los servicios al usuario final, siendo este desde un individuo hasta un gran corporativo.

El modelo de negocio de la nube pública permite que se puedan ofertar servicios de manera gratuita, teniendo retorno en la inversión mediante otros métodos de obtención de ingresos, tales como publicidad, bases de datos, etc.

Debido a la cantidad y variedad de usuarios de la nube pública, en la mayoría de los casos, la información se encuentra en varios CPD, limitándose la responsabilidad del proveedor a la que éste determine en los términos y condiciones aceptados por el usuario.

Por lo general la nube pública es utilizada por usuarios individuales o instituciones/ corporaciones con operaciones locales, de poca facturación y/o que prestan servicios generales que no requieren un nivel alto de privacidad para su información.

[16] El código de conducta de la Unión Europea sobre eficiencia energética en *Datacenters* se publicó el 30 de octubre de 2008. Disponible solamente en inglés en http://iet.jrc.ec.europa.eu/energyefficiency/ict-codes-conduct/data-centres-energy-efficiency

2.2.2 Nube privada

Como su nombre lo indica, se trata de un espacio virtual y físico dedicado en exclusiva a un cliente y los usuarios que este determine. La nube privada permite mayor control en la administración de la nube, optimizando las características de autoservicio, acceso a la red y elasticidad. La nube privada es un entorno diseñado y gestionado a la medida del cliente/ usuario.

El concepto de privado se refiere al funcionamiento de un CPD "exclusivo" y el cliente es quien asume el costo del *hardware*, el cual podrá estar físicamente dentro de las instalaciones del cliente (*on-premise),* o fuera de éstas (*off-premise).* En caso de tener el CPD en las instalaciones de la corporación, es el equipo de empleados del departamento de sistemas, quienes administran, mantienen y resguardan el *hardware*. De manera contraria, si el *hardware* está resguardado físicamente por un tercero, éste se obliga a permitir el acceso únicamente a los usuarios que autorice el cliente, teniendo mayor responsabilidad en la seguridad de la información.

La nube privada es un modelo eficaz para organizaciones con grandes volúmenes de operación o para aquellas que requieren mayor privacidad en sus actividades desde la nube y en la seguridad de su información.

El modelo de negocio de la nube privada es costosa para el cliente, en virtud que es el cliente el responsable de todos los gastos que se generen por mantener la privacidad y control de la información y su operación, incluyendo la adquisición, mantenimiento y resguardo del *hardware;* implementación y monitoreo de medidas de seguridad; instalación, asistencia técnica; y actualizaciones del *software* y aplicaciones que permitan el uso de la nube.

En caso que algún proveedor preste el servicio de nube privada, la ganancia de éste, se basará en los servicios que "efectivamente" sean prestados (por ejemplo la renta de la nube) sin otros métodos de generación de ingresos, tales como venta de datos, publicidad, etc.

La nube privada es empleada por corporaciones cuya operación permite absorber el costo de implementación, así como sectores públicos y privados críticos, tales como instituciones financieras, servicios médicos, aduanas, entidades de

impartición de justicia, etc., a razón que la información que está en su posesión tiene mayor demanda de confidencialidad.

2.2.3 Nube híbrida o mixta

Este modelo permite combinar las ventajas de la nube pública y privada, minimizando los riesgos de la nube pública y los costos de la nube privada, ya que la nube híbrida es un punto intermedio entre un sistema “a la medida” y un sistema abierto como la nube pública, mediante el cual dependiendo las necesidades del cliente, se segmentarán los procesos críticos y confidenciales, a efecto de determinar cuáles estarán en la nube privada para ser operados y controlados por los usuarios que determine el cliente, dejando los procesos menos riesgosos en la nuble pública.

La nube pública permite operar con bajos costos y con menos restricciones de acceso ya que se puede conectar desde internet, sin embargo, su principal desventaja es la opacidad en el manejo de la información/ operación del cliente, debido a que los recursos son proporcionados por un tercero, el cual tiene el control absoluto, limitándose la participación del cliente a reportes y - como excepción- auditorías periódicas.

Por lo anterior, las aplicaciones no fundamentales o también conocidas como *non-core* y las operaciones no críticas, se administran desde la nube pública.

De manera contraria, en la nube privada el cliente es el propietario de los recursos (ya sea *on-premise off-premise*) lo que permite mayor control y confidencialidad, incluso los accesos están restringidos a una red local o por internet mediante un sistema de autenticación más estricto como es la Red Privada Virtual (VPN)[17]. Debido al alto costo de operación, sólo las actividades críticas e información confidencial se resguardan en este modelo de nube.

La nube híbrida es un modelo utilizado por clientes y/o corporaciones que operan a escala mediana así como entidades públicas que por la variedad de

[17] La red privada virtual (VPN) es una red privada construida dentro de una infraestructura de red pública (internet). Se usan redes privadas virtuales para conectar en forma segura a usuarios remotos a través de accesos a internet proporcionados las redes públicas de telecomunicaciones. Las redes privadas virtuales proporcionan el mayor nivel posible de seguridad, protegiendo los datos que pasan por la red privada virtual contra accesos no autorizados.

procesos, no requieren que toda su operación se encuentre en “estricta confidencialidad y seguridad”. Así mismo, en la mayoría de ocasiones, la nube híbrida es el paso previo para habilitar una nube privada, ya que la migración de información e implementación en la operación a la nube privada es un proceso no inmediato que no siempre requiere desde el inicio la más alta privacidad y control, teniendo como opción trabajar desde una nube híbrida durante su implementación con la finalidad de disminuir costos.

2.3 Ventajas del uso de la nube

Dependerá del tipo de nube (pública, privada o mixta) las ventajas de implementar su uso. Sin embargo, de manera general, se pueden enunciar las siguientes:

Accesibilidad. Por tratarse de un servicio proveído a través de internet, es posible acceder desde cualquier parte del mundo sin límite de horario (24 horas 365 días), por lo que en caso de contratar cualquier servicio relacionado a la nube con costo para el cliente, se puede solicitar al proveedor que garantice la accesibilidad mediante el pago de una fianza.

Se puede reforzar la seguridad al acceder al limitar el acceso a determinadas regiones mediante geo-bloqueos que impiden el acceso de los números IP distintos a la zona geográfica autorizada o solicitar medidas de autenticación tales como conexiones VPN y/o contraseñas de acceso.

La nube permite que se acceda a la información desde cualquier dispositivo, incluyendo computadoras de escritorio, portátiles y móviles, para lo cual se crean las aplicaciones con códigos PHP, HTML5 y CSS3 que identifican el dispositivo y ajustando la estructura visual para presentar la información al usuario de manera más amigable.

Menor costo. Al no requerir inversión en discos duros por equipo, se reduce el costo de adquisición de soportes físicos, mantenimiento y servicios, así como los honorarios por personal de asistencia técnica al usuario, toda vez que funcionando el servidor cualquier falla del usuario se reduce a problemas con el equipo de acceso y no al servidor, requiriendo sólo la sustitución o reparación del punto de acceso.

En caso de nube pública e híbrida, el gasto inicial es mínimo o nulo, ya que el esquema de negocio permite operar sin gran inversión, devengando

mensualmente la renta por el servicio y responsabilizando al proveedor de los gastos de servicio técnico y mantenimiento.

Por otra parte, la nube permite el máximo aprovechamiento de recursos, ya que solo se contratan los servicios que se requieren (espacio de almacenamiento, encriptado, transferencia de archivos FTP, etc.), teniendo posibilidad de incrementarlos o disminuirlos de manera inmediata según las necesidades de la operación. Esto representa una herramienta fundamental para controlar gastos en una crisis o para crecer de manera asertiva sin afectar el flujo de efectivo.

Al no requerir una gran inversión inicial, los clientes que no cuenten con recursos para la adquisición de infraestructura, tendrán acceso a desarrollos tecnológicos que les permitan ser más competitivos al hacer más eficientes sus procesos y operaciones, teniendo posibilidad de competir en igualdad de condiciones con organizaciones de cualquier tamaño.

Seguridad. Aunque la seguridad no sea controlada por el cliente, las posibilidades de que éste tenga mejor resguardada la información son mayores, toda vez que los proveedores deben cumplir con estándares mínimos de seguridad por razones de competencia y disposiciones legales, tales como acceso restringido, copias de seguridad, control en la migración de información, etc.

Así mismo, un cliente pequeño puede beneficiarse de los recursos físicos y financieros que invierta el proveedor para resguardar y controlar amenazas a la información de clientes con mayores requerimientos de seguridad, toda vez que las medidas de seguridad se aplican de manera general, particularizando solamente aspectos peculiares en el manejo de información altamente confidencial (datos personales sensibles, secretos industriales, etc.).

Respaldos. Debido a que ningún proveedor de servicios de la nube, garantiza la integridad de la información del cliente, los proveedores generan respaldos constantes con la finalidad de recuperar cualquier información faltante, representando una ventaja ya que es poco frecuente que el cliente por su propia cuenta genere respaldos de su información.

La limitación de la responsabilidad del proveedor obedece a un motivo técnico, toda vez que es imposible evitar que por fallas en el procesamiento se pierda información.

Escalabilidad. El procesamiento de la información se realiza desde la nube a través del equipo de cómputo o dispositivo móvil, por lo que la capacidad de ejecución del dispositivo de acceso que se requiere es mínima.

Además del beneficio económico por una menor inversión en los dispositivos de los usuarios, en caso de tener requerimiento de procesos más complejos, se trabaja solamente en el *hardware* de la nube, permitiendo que se actualice de manera inmediata en toda la red de usuarios, siendo obligación del proveedor dicha actualización.

Lo anterior también aplica para las medidas de seguridad, que al incrementarse en la nube, en automático se aplica para todos los usuarios.

Como consecuencia de la "centralización" de la operación de procesos y funcionalidades en la nube, se pueden incrementar o disminuir los servicios de manera inmediata y general para todos los usuarios en un solo momento, permitiendo una prestación de servicios ilimitado (almacenamiento, procesamiento, funcionalidad, herramientas, recursos, etc.)

Procesos administrativos más eficientes. En cualquier proceso de implementación de la nube, se realiza un levantamiento de necesidades del cliente, detectando métodos, políticas y procedimientos internos a efecto de determinar la interacción de los usuarios con la nube, facilitando la detección de malas prácticas que afectan la productividad, manejo incorrecto de la información, fallas de seguridad en la confidencialidad, etc.

Adicionalmente, al tener automatizados los procesos mediante la nube y delegando responsabilidades de operación, seguridad y mantenimiento del sistema en la nube, el cliente puede enfocar recursos y esfuerzos a los aspectos del negocio principal.

2.4 Desventajas del uso de la nube

Como cualquier tecnología, también existen inconvenientes en la nube. Dichos inconvenientes se pueden minimizar a través de la nube híbrida y desde los

acuerdos contractuales entre el proveedor y el cliente. Las principales críticas a la nube son:

Pérdida de propiedad y privacidad. El cambio de paradigma de soportes físicos a virtuales conlleva escepticismo en los líderes de las organizaciones respecto a la implementación de la nube, toda vez que al no contar con el soporte físico se genera la sensación de pérdida de la propiedad y privacidad.

La sensación de control deviene del acceso al soporte físico, por lo que al no estar visible, se presupone que la información resguardada en la nube es vulnerable a ser divulgada y traficada sin consentimiento del cliente, y aunque esto es cierto materialmente, en el entorno legal el uso de la información resguardada sin autorización del cliente generará responsabilidad civil o penal al proveedor del servicio según los acuerdos contractuales celebrados entre las partes y la legislación aplicable.

Jurisdicción. En caso de contratar servicios de la nube cuyos servidores se localicen fuera del territorio del cliente, se estaría sujeto a las leyes y jurisdicción del servidor, por lo que añade cargas legales al cliente, quien por desconocimiento, podría infringir en incumplimientos a las regulaciones aplicables en el extranjero.

Dependencia al proveedor. La falta de control por parte del cliente se vuelve palpable en la operación diaria de la nube, toda vez que hay dos elementos indispensables para su ejecución, siendo uno de carácter contractual (la provisión del servicio) y otro de índole tecnológica (el acceso a internet).

El proveedor del servicio mantiene el control durante los tres momentos claves de su operación: implementación, operación y mantenimiento, lo que agudiza la percepción del poco control y movilidad del cliente para resolver cualquier incidente derivado de la nube que puede consistir en aspectos técnicos como fallas, problemas de acceso, riesgos de seguridad, etc.; y/o aspectos comerciales como nuevos proveedores, cancelación de contrato, etc.

Si el contrato con el proveedor no prevé sanciones en caso de suspensión del servicio, éste podrá a su discreción suspender el acceso, afectando la operación del negocio del cliente, generando cuantiosas pérdidas que incluso pueden ser irreparables (por ejemplo transacciones bancarias, expedientes clínicos, etc.).

Las condiciones del contrato deberán ser asertivas desde el inicio, obligando al proveedor a realizar las actualizaciones o mejoras en las aplicaciones e infraestructura según el avance tecnológico, toda vez que por tratarse de contratos de tracto sucesivo, existe poca capacidad de renegociación por la dependencia del cliente hacia el proveedor.

Dependencia de la conexión a internet. La conexión a internet es un elemento básico para el funcionamiento de la nube, por lo que la suspensión del servicio, ya sea por razones físicas del proveedor de telecomunicaciones o incluso la omisión en el pago, evitan el acceso a la nube, afectando las operaciones del negocio y generando pérdidas cuantiosas.

También la calidad del servicio se vuelve un factor a considerar, ya que una conexión inestable, lenta o intermitente, genera problemas de conexión con los servidores de la nube propiciando la pérdida de información o error en la generación de procesos.

Poca intervención del cliente en las medidas de seguridad. Aunque la responsabilidad de la implementación y funcionamiento adecuado de las medidas de seguridad será del proveedor de servicios de la nube, las vulneraciones a la seguridad afectarán de manera directa al cliente, exponiendo su seguridad financiera sin posibilidades a resarcimientos porque las condiciones del mercado de servicios de nube limitan el monto de la responsabilidad al valor del contrato.

Lo anterior genera mayor reticencia de la migración a la nube, ya que el cliente no puede intervenir en la seguridad, pero al mismo tiempo es el afectado, dejando su información vulnerable a robos, divulgación y mal uso, exponiendo no solo el patrimonio físico de la empresa sino el patrimonio moral de la misma, el cual se integra por la percepción de sus consumidores.

Así mismo, si no se pacta en el contrato las obligaciones de llevar a cabo respaldos de la información, quedará al arbitrio y buena voluntad del proveedor el generarlos con la periodicidad necesaria.

No obstante lo anterior, se pueden adoptar medidas de seguridad sin requerir la intervención del proveedor, tales como cifrar la información que se almacenará en la nube, sistema de verificación de acceso en dos pasos, respaldo de información

clave en discos duros locales, conocer la ubicación física de los servidores del proveedor, instalar antivirus y *firewalls* en los dispositivos que accederán a la nube.[18]

[18] Hipertextual, "Cómo mejorar la seguridad de tus archivos en la nube", España, 2014. http://hipertextual.com/archivo/2014/09/seguridad-nube/. Fecha de consulta 13 de mayo de 2016.

Capítulo 3

Propuesta de implementación del uso de la nube por el departamento jurídico de empresa para la contratación de personal

Capítulo 3. Propuesta de implementación del uso de la nube por el departamento jurídico de empresa para la contratación de personal

Cualquier unidad económica requiere servicios legales para dotar de formalidad a sus operaciones y así evitar contingencias legales.

Dependiendo los intereses y recursos de la empresa, los servicios jurídicos podrán ser prestados por consultoría externa, abogados internos o sistema mixto que combine la operación diaria supervisada por abogados internos y servicios externos para asuntos especializados.

La operación legal de cualquier empresa se puede dividir en servicios legales de negocio, operación y litigio, con la siguiente subdivisión:

1. Servicios legales de negocio:
   a) Contratación.- Proveedores, clientes y comercialización por comercio electrónico.
   b) Corporativo.- Actas constitutivas, poderes, documentación de inversiones, emisiones de deuda, fideicomisos, inmuebles, administración legal de inmuebles, etc.
2. Servicio legales de operación:
   a) Contratación de servicios de suministro.
   b) Recursos humanos.- Contratación de personal, previsión social y bajas de empleados.
   c) Regulatorio.- Obtención de permisos y autorizaciones, cumplimiento de normas oficiales, cumplimiento de obligaciones fiscales, actos relacionados con autoridades administrativas, entre otros.
3. Litigio
   a) Cobranza. - Extrajudicial y judicial.
   b) Mercantil y Civil.
   c) Penal. - Averiguaciones previas y procesos penales.

Figura 3. Servicios legales en empresa

Fuente: Elaboración propia de acuerdo al organigrama estándar de un departamento jurídico de empresa

2.5 Propuesta de modelo de implementación de nube

La opción “ideal” de nube para almacenar y operar las actividades jurídicas es la nube privada por motivos de confidencialidad y control de información, sin embargo, los costos de servidores, servicios técnicos y seguridad, en la mayoría de los casos, no son justificables en virtud que los servicios legales son un área que genera gastos en lugar de generar ingresos.

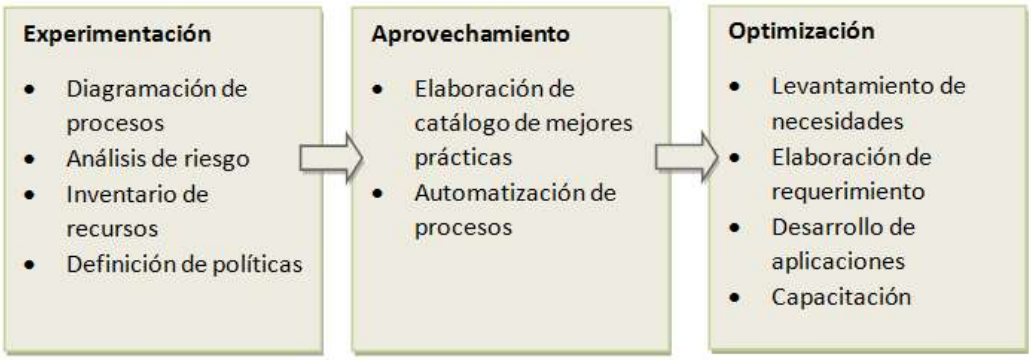
En contraste, la nube pública representa menores costos y acceso a más servicios, pero expone información que puede suponer una ventaja competitiva para la empresa e incrementa la dependencia con el prestador del servicio, disminuyendo el control respecto a la administración de la información legal de la empresa, toda vez que, a diferencia de la nube privada, el acceso a las unidades de almacenamiento es operado directamente por el proveedor.

Por lo anterior, dependiendo de los recursos de la empresa, el modelo de nube más adecuado para un área de servicio como el departamento jurídico, es el sistema mixto o híbrido, que permite aprovechar los beneficios de ambos tipos de

nube y que con un análisis a detalle de las operaciones legales, se podrán disminuir de manera considerable las desventajas de cada modelo.

Para realizar una implementación exitosa de la nube se puede llevar a cabo el modelo de las tres fases[19] que consiste en experimentación, aprovechamiento y optimización de la nube con la adopción de estándares de seguridad tecnológica para cubrir las necesidades de la operación de un departamento jurídico de empresa con enfoque a la protección de datos personales.

Figura 4. Propuesta adaptada del modelo de tres fases



Fuente: Elaboración propia de acuerdo al modelo de tres fases para la implementación de cómputo en la nube propuesto por *Search Data Center*

Fase de experimentación. Consiste en identificar los requerimientos básicos para determinar el tipo de nube. En esta fase, la nube tiene como finalidad de ser utilizada como repositorio a través de la ejecución de aplicaciones de acceso. Esta fase se integra de cuatro etapas:

a) Diagramación de procesos. Es el primer paso para conocer el detalle de la operación del departamento jurídico. Identificar los procesos es la base para llevar a cabo una implementación funcional que permita maximizar el uso de los recursos. Son los planos del proyecto.

[19] Del Vecchio, José et al., "La computación en la nube: un modelo para el desarrollo de las empresas", *Prospect,* Colombia, vol. 13 no. 2, 2015, pp. 81-87.

b) Análisis de riesgo. Considerando que la prioridad en la implementación de la nube es garantizar la protección de los datos personales, se propone utilizar la Metodología de Riesgo BAA, la cual es sugerida por el INAI y que consiste en estimar el riesgo según el tipo de dato, tipo de acceso y tipo de entorno con evaluación de las medidas de seguridad habilitadas[20].
c) Inventario de recursos. Posiblemente existan herramientas previamente implementadas en la operación comercial de la empresa que puedan ser aprovechadas por el departamento jurídico, por lo que realizar un inventario previo a adquirir cualquier recurso adicional evita gastos innecesarios.
d) Definición de políticas. Las políticas son la normativa interna de cualquier empresa y se encargan de establecer los criterios de operación de la organización, por lo que cualquier actividad en que intervenga el departamento jurídico, deberá contar con lineamientos claros que definan los parámetros de actuación del equipo legal para que coadyuve con la supervisión y auditoría de la operación comercial de la organización.

Fase de aprovechamiento. Es la fase que permite rediseñar los procesos para identificar el potencial del uso de la nube. Se integra por dos etapas:

a) Elaboración de catálogos de mejores prácticas. Consiste en enlistar las recomendaciones que mejoran la operación del departamento jurídico y que por su naturaleza no requieren de obligatoriedad para convertirse en políticas.
b) Automatización de procesos. Cuando el proceso ha sido diagramado es posible identificar aquellas actividades que pueden ejecutarse por sí mismas al cumplir con alguna condición, lo cual permite disminuir los errores humanos y previene cualquier daño al detener el proceso por actividades faltantes o no autorizadas. Tratándose de datos personales, la automatización es una herramienta fundamental para la gestión adecuada de los mismos, ya que si se cuenta con procesos eficientes y aplicaciones acordes a los estándares de seguridad, se puede garantizar el cumplimiento

[20] Las medidas de seguridad que se utilizaron como referencia son las determinadas en ISO/IEC 27002. Recomendaciones de las Mejores Prácticas en la Gestión de la Seguridad de la Información.

de los deberes y principios en el tratamiento de datos personales, en particular en las actividades de obtención de consentimientos, actualización de información, bloqueo de datos y ejercicio de derechos ARCO.

Fase de optimización. Es la última fase de la implementación y es el momento en que se concreta la evolución de la nube, pasando de un simple repositorio a una herramienta de gestión. En esta fase se integran las aplicaciones, que son los sistemas que se ejecutan en la nube. Se integra por las siguientes etapas:

a) Levantamiento de necesidades. Al igual que la diagramación de procesos es la base de cualquier implementación de nube, el levantamiento de necesidades es la base para explotar el potencial del uso de nube a través de las aplicaciones, toda vez que éstas serán los medios por los cuales se ejecutarán las operaciones del departamento jurídico. Un levantamiento adecuado de los objetivos y funciones esperadas de las aplicaciones permite disminuir los tiempos de trabajo, mejora la supervisión e incluso se puede interfazar con otros sistemas para condicionar las operaciones comerciales de la organización al previo cumplimiento de los requerimientos legales establecidos por el departamento jurídico.
b) Elaboración de requerimiento. Existen aplicaciones en el mercado que ofrecen satisfacer las necesidades operativas del cliente, sin embargo, en la mayoría de los casos, se adquiere la licencia de la aplicación pre-existente y se contratan servicios de desarrollo para ajustar el programa a la operación del cliente. Otra opción consiste en desarrollar una aplicación desde cero para cumplir con las necesidades especializadas del cliente. En ambos casos, es necesario preparar el requerimiento, que consiste en el documento que señala la funcionalidad y los alcances del desarrollo de la aplicación.
c) Desarrollo de aplicaciones. Se trata de la construcción de la aplicación, incluyendo fases de prueba y ajustes.
d) Capacitación. La implementación de nuevas formas de trabajo requiere capacitación a los usuarios para explotar el potencial de la aplicación desarrollada. En ocasiones, por tratarse de la última etapa de implementación, se resta importancia a la capacitación del personal que

utilizará las aplicaciones y la nube, por lo que se propone reforzar la capacitación a través del involucramiento de todo el equipo durante las tres fases con la finalidad de crear un sistema amigable e intuitivo para el usuario, disminuyendo así el tiempo de capacitación y la resistencia al cambio por contar con una nueva forma de operación.

2.6 Medidas de seguridad

Cualquiera que sea el modelo de nube adoptado, para asegurar el cumplimiento de disposiciones en el tratamiento de los datos personales, se deberá cumplir con las medidas de seguridad aplicables según los resultados del análisis de riesgo.

Para facilitar esta tarea, el INAI publicó en 2013 las “Recomendaciones en materia de seguridad de datos personales” que se basa en el modelo “Planificar- Hacer- Verificar- Actuar” el cual se integra por nueve pasos agrupados en 4 fases. Se trata de un modelo completo que audita, complementa, ejecuta y promueve la mejora continua de las medidas de seguridad relacionadas con el tratamiento de datos personales.

Además, los sujetos involucrados en el tratamiento de datos, pueden apoyarse de certificaciones que validan el cumplimiento de los principios y deberes en la gestión de sus procesos. Para estos efectos el INAI emitió en 2015 la “Tabla de Equivalencia Funcional entre Estándares de Seguridad y la LFPDPPP, su Reglamento y las Recomendaciones en Materia de Seguridad de Datos Personales” que contiene un análisis del cumplimiento de las disposiciones de las leyes en la materia por cada modelo de certificación, destacando que existen dos estándares que cumplen en su totalidad con la normativa en datos personales: ISO/IEC 27001 Tecnologías de la Información- Requerimientos e ISO/IEC 27002 Tecnologías de la información- Código de prácticas para la administración de la seguridad.

La certificación en cualquiera de los dos estándares garantiza que los procesos cumplen con los principios y deberes durante el tratamiento de los datos personales, por lo que deberán incluirse en el proceso de implementación de nube a efecto de ajustar los procesos, políticas y requerimientos de las aplicaciones.

2.7 Riesgo por el tipo de dato

Para identificar las medidas de seguridad que deberán ser aplicables, es necesario realizar un análisis de riesgo, recomendándose la metodología de análisis de riesgo BAA que ha sido validada por el INAI.

El análisis de riesgo incluye entre otros valores, el riesgo por el tipo de dato, el cual se integra, por el riesgo inherente de los datos más el volumen de los titulares, identificando cuatro categorías de riesgo inherente: reforzado, alto, medio y bajo.

a) Riesgo inherente reforzado. Datos personales de figuras con alta exposición pública y/o personas cuya profesión está relacionada con la impartición de justicia y seguridad nacional.

b) Riesgo inherente alto. Datos personales sensibles.

c) Riesgo inherente medio. Datos que permiten conocer la ubicación física de la persona y/o que permita volver identificable a otra persona y/o datos personales financieros o patrimoniales y/o datos de autenticación y/o datos jurídicos.

d) Riesgo inherente bajo. Datos de contacto y los que no formen parte de las categorías anteriores.

Por lo que hace al volumen de los titulares, se cuentan con cinco niveles que se interrelacionan con el riesgo inherente del dato:

a) Nivel 1

- Riesgo inherente de los datos es bajo, sin importar el número de titulares.
- Riesgo inherente medio y hasta 5,000 titulares.
- Riesgo inherente alto y hasta 500 titulares.

b) Nivel 2

- Riesgo inherente medio y hasta 50,000 titulares.
- Riesgo inherente alto y hasta 5,000 titulares.

c) Nivel 3

- Riesgo inherente medio y 50,000 titulares en adelante.
- Riesgo inherente alto y 5,000 titulares en adelante.

d) Nivel 4

- Riesgo inherente reforzado y hasta 5,000 titulares.

e) Nivel 5

- Riesgo inherente reforzado y 5,000 titulares en adelante.

2.8 Propuesta de implementación de nube en proceso de contratación de personal

La estrategia de implementación de la nube debe ser un proyecto a medida de las necesidades de las operaciones de la empresa y del departamento jurídico que considere los recursos asignados por la organización. Sin embargo, existen procesos que por su naturaleza son homogéneos y tendrán solo algunos ajustes dependiendo el tamaño de los equipos de trabajo involucrados, siendo uno de ellos, la contratación de personal, la cual dependiendo el volumen de la plantilla y los intereses legales de la empresa, se puede llevar a cabo con tres variantes: Contratación directa, Selección de personal a través de un prestador de servicios de recursos humanos o la contratación a través de un tercero- *outsourcing*.

De manera independiente al modelo de contratación que adopte la organización, cualquier implementación de la nube que pretenda ser eficiente en el cumplimiento de la protección de los datos personales, deberá contar con los procesos diagramados de la operación y el análisis de riesgos por el tipo de dato.

A continuación se desglosan las actividades que en el proceso de selección de personal involucran el tratamiento de los datos personales con las recomendaciones para el cumplimiento de los principios y deberes, y el tipo de nube que puede utilizarse.

2.8.1 Búsqueda de candidatos

Cualquier organización requiere consultar bancos de información utilizando criterios de búsqueda relacionados con datos personales.

En caso que los bancos de información sean propios, es decir, que los interesados proporcionen de manera directa (principio de lealtad) su información en la plataforma de la empresa (Ej. Bolsa de trabajo de *Coca Cola Company,* grupo Alsea, etc.), se deberá solicitar sólo aquella información indispensable para identificar el perfil del candidato: nombre, fecha de nacimiento, sexo, datos de

contacto, formación académica y experiencia profesional (principio de proporcionalidad). Es importante omitir cualquier requerimiento de información relativa a domicilio, ingresos y pasatiempos ya que en caso contrario, se incrementará el nivel de riesgo y se deberá cumplir con los requisitos adicionales establecidos para el tratamiento de datos personales patrimoniales y sensibles. El aviso de privacidad que se despliegue durante la carga de información deberá señalar que los datos personales serán tratados para fines de selección de personal (principio de información) y que la disponibilidad en la base de datos tendrá una vigencia de 18 meses (principio de calidad). La nube que puede utilizarse bajo estas recomendaciones, es la nube pública con accesos permitidos sólo a las personas involucradas en la selección de personal.

Si por el contrario, los bancos con información de candidatos son proveídos por un tercero (Ej. OCC, Linkedin, etc.), se deberá verificar que el aviso de privacidad de los terceros permite la transferencia de datos personales y se deberá disponer una cláusula en los contratos con los proveedores que los obligue a obtener las autorizaciones necesarias para la transferencia de los datos personales (principios de legalidad y lealtad). En estos casos, es recomendable obtener sólo aquella información indispensable para identificar la viabilidad del candidato, sin embargo, entendiendo que la información es recabada en formatos pre-establecidos por un proveedor, se recomienda evitar la creación de bases de datos propias con la información proporcionada por el proveedor para no reproducir datos personales sensibles y patrimoniales. También se sugiere eliminar cualquier respaldo de la información de los candidatos descartados dentro de las veinticuatro horas siguientes y poner a disposición del público en general, un aviso de privacidad por la obtención indirecta de datos personales (principio de consentimiento). En este caso, para la empresa es irrelevante el modelo de nube para el banco de datos, toda vez que éstos están bajo el control del proveedor, sin embargo el manejo temporal de los datos de candidatos por el personal de la empresa podrá realizarse en nube pública con accesos restringidos.

2.8.2 Entrevistas

El contacto personal con los candidatos se materializa con las entrevistas, que podrán ser de manera remota (por teléfono o video llamada) y/o presencial, y el número de entrevistas dependerá de lo exhaustivo que sea el proceso de selección. Se recomienda que en el proceso se realicen sólo entrevistas esenciales para determinar la viabilidad del candidato para evitar obtener datos que no sean acordes a las finalidades del tratamiento. Los entrevistadores deberán ser capacitados para que sólo obtengan aquella información que sea relevante para conocer el perfil del candidato.

La contratación del personal depende tanto de elementos objetivos (experiencia profesional, preparación académica, etc.) como de elementos personales (personalidad, valores, etc.), por lo que es usual que en las entrevistas se tenga acceso a información íntima del candidato que puede consistir en datos personales sensibles. En estos casos, se recomienda que los entrevistadores no tomen notas ni lleven a cabo la creación de bases con los datos personales sensibles del candidato, tales como pasatiempos, religión, ideologías, etc.

Por otra parte, es usual que exista interés en crear bases de información con datos personales patrimoniales, tales como ingresos en el empleo anterior, gastos personales y expectativas salariales, por lo que sí es el caso, se deberá recabar el consentimiento expreso por el titular de manera previa al tratamiento de los datos.

Cualquier soporte físico que contenga información recabada en entrevistas deberá descartarse dentro de las veinticuatro horas siguientes a que se descarte el candidato.

Se recomienda evitar el almacenar información obtenida en entrevistas en aplicaciones utilizadas para selección de personal.

2.8.3 Exámenes

Evaluar al candidato es un requisito en cualquier gestión exitosa de contratación de personal, sin embargo, es la etapa más riesgosa para el tratamiento de datos, toda vez que su objetivo es obtener datos íntimos de candidato, exceptuando el examen de conocimientos cuya finalidad es obtener datos objetivos de la capacidad del candidato. Por lo regular, los exámenes médicos, psicométricos y socio-económicos

son prestados por proveedores que obtienen los datos por cuenta de la empresa, convirtiéndose en encargados. Para disminuir el riesgo, se deberán revisar los aspectos a evaluar para descartar aquellos que no sean fundamentales para determinar la viabilidad del candidato.

Los contratos celebrados con los encargados deberá obligarlos a tomar las medidas de seguridad necesarias durante el tratamiento de los datos recabados y que informen cualquier vulneración a los sistemas de seguridad.

De ser posible, se recomienda que la remisión de información se realice en las aplicaciones de la empresa, a efecto de controlar los accesos a dicha información.

El titular de los datos deberá tener a su disposición, previo a que le realicen los exámenes, el aviso de privacidad que informe de manera clara que el tratamiento de sus datos será para determinar la coincidencia de su perfil con la vacante y que dichos datos estarán disponibles durante el periodo que tenga relación directa con la empresa. Por tratarse de datos personales sensibles y patrimoniales, se deberá obtener el consentimiento expreso y por escrito.

En caso que se descarte al candidato o cuando termine la relación laboral con el mismo se deberán bloquear de inmediato los datos personales correspondientes.

Se recomienda que los resultados de exámenes se almacenen en nube privada o en nube pública con servicios adicionales de seguridad y acceso permitido sólo a usuarios con privilegios gerenciales (principio de responsabilidad y deberes de confidencialidad y seguridad).

Existe un esquema que permite evitar cualquier contacto con datos personales sensibles y patrimoniales por parte de la empresa: la validación del candidato por un proveedor.

Este esquema es común cuando la contratación del personal la lleva a cabo un proveedor- *outsourcing*, sin embargo, en caso que no sea del interés de la empresa que la administración de los recursos humanos recaiga fuera de la administración de la propia empresa, se puede contratar solo la etapa de validación de candidatos.

La validación del candidato por parte de un proveedor consiste en que este último, concentra los resultados de los exámenes realizados a los candidatos, ya sea que él mismo realice los exámenes o que sólo recabe la información, cotejándolos contra los valores mínimos proporcionados de la empresa de manera previa, obligándose a informar únicamente si el candidato cumplió con los parámetros solicitados por la empresa, evitando así participar en el tratamiento de los datos personales proporcionados por cualquier candidato.

En el contrato celebrado con el prestador deberá especificar los alcances y garantías otorgadas por quien valida a los candidatos, con posibilidad de auditar la información en caso que la empresa así lo requiera.

La validación de los candidatos se deberá proporcionar en formatos previamente establecidos por la empresa, los cuales deberán limitarse a resultados positivos o negativos, sin incluir detalles de los resultados de los exámenes.

2.8.4 Creación de expediente

Una vez seleccionado el candidato, se concluye el proceso de selección con la entrega de documentos, que deberán consistir en sólo aquellos que sean necesarios para comprobar la información proporcionada por el candidato (principio de proporcionalidad).

En el contrato se deberán incluir cláusulas con autorización del tratamiento de datos personales acordes al aviso de privacidad de la empresa, confidencialidad y obligaciones de actualización de datos personales (principio de calidad).

El expediente podrá ser físico y/o digital. El expediente digital podrá estar en un repositorio simple o como parte de alguna aplicación especializada para la gestión del personal y/o en el sistema de nómina. El resguardo del expediente digital puede ser en nube privada o en nube pública con recursos adicionales de seguridad y accesos controlados.

En resumen, las recomendaciones para el proceso de contratación de personal son:

Actividad: Búsqueda de candidatos.

Propuesta de nube: Nube pública con acceso solo a usuarios.

Recomendaciones:

Bancos de información propios:

- Solicitar sólo información necesaria.
- Evitar requerir datos personales patrimoniales y sensibles.
- Tratamiento de datos personales para fines de selección de personal.
- Vigencia de las bases de datos de 18 meses.

Bancos de información de terceros:

- Verificar que el aviso de privacidad permite la transferencia de datos.
- Cláusula que obliga a los proveedores a obtener autorización para transferencia de datos personales.
- No crear bases de datos propias con información del proveedor.
- No reproducir datos personales sensibles y patrimoniales.
- Eliminar información de los candidatos descartados dentro de las 24 horas siguientes.
- Aviso de privacidad a disposición del público en general por la obtención indirecta.

Actividad: Entrevistas.

Tipo de nube: N/A.

Recomendaciones:

- Identificar sólo entrevistas esenciales.
- Capacitar a entrevistadores para obtener información relevante.
- Evitar tomar notas y crear bases con los datos personales sensibles del candidato.
- Recabar autorización expresa para crear bases de información con datos personales patrimoniales.
- Descartar soportes físicos con información recabada en entrevistas dentro de las 24 horas siguientes a que se descarte al candidato.
- No almacenar información obtenida en entrevistas en la nube.

Actividad: Exámenes.

Tipo de nube: Nube privada o en nube pública con servicios adicionales de seguridad y acceso permitido sólo a usuarios con privilegios gerenciales.

Recomendaciones:

- Descartar aspectos a evaluar irrelevantes para la posición.
- Obligar por contrato a los encargados a tomar medidas de seguridad suficientes e informar vulneraciones de los datos.
- Remisión de información a través de las aplicaciones de la empresa.
- Aviso de privacidad claro con consentimiento expreso y por escrito para tratamiento de datos personales sensibles y patrimoniales.
- Bloquear los datos de manera inmediata en caso que se descarte al candidato o cuando termine la relación laboral.
- Implementar esquema de validación de exámenes por parte de un proveedor.
- Establecer por contrato, alcances y garantías del proveedor que valide a los candidatos.
- Establecer formatos de validación.

Actividad: Creación de expediente.

Tipo de nube: Nube privada o en nube pública con recursos adicionales de seguridad y accesos controlados.

Recomendaciones

- Solicitar solo documentos necesarios para comprobar la información del candidato.
- En el contrato laboral incluir cláusulas con autorización del tratamiento de datos personales acordes al aviso de privacidad de la empresa, confidencialidad y obligaciones de actualización de datos personales.

2.8.5 Análisis de riesgo por el tipo de dato

Del proceso de contratación y el análisis de las actividades que lo integran, se desprende que los datos personales involucrados implican riesgo inherente bajo, medio y alto, por lo que dependiendo del volumen de titulares que tenga la organización, se estaría en valores de riesgo por dato en escala del 1 al 3, tal como se desglosa a continuación:

Cuadro 1. Análisis de riesgo

Actividad	Datos personales a recabar	Riesgo inherente	Riesgo por el tipo de dato			
Búsqueda de candidatos	Nombre, datos de contacto, experiencia profesional y trayectoria académica	Bajo	1	1	1	1
Entrevistas	Ingresos, prestaciones y pretensiones económicas	Medio	1	1	2	3
	Información de familiares, amigos y colegas	Medio	1	1	2	3
Exámenes	Entorno económico y social	Alto	1	2	3	3
	Estado de salud	Alto	1	2	3	3
	Estado mental	Alto	1	2	3	3
Creación de expediente	Comprobante de domicilio	Bajo	1	1	1	1
	Acta de nacimiento	Bajo	1	1	1	1
	Documentación de prestaciones sociales para familiares	Medio	1	1	2	3
		Volumen de los titulares	<500	< 5 K	< 50 K	50 K >

Fuente: Elaboración propia de acuerdo a la metodología BAA del INAI

2.8.6 Medidas de seguridad recomendadas

Considerando el valor por el riesgo del dato, se sugieren las siguientes medidas de seguridad para la implementación de la nube:

a) Riesgo nivel 2.

- Determinar políticas de seguridad aprobada por el departamento jurídico y deberá ser comunicada a todos los empleados y terceras partes relevantes.
- Las políticas de seguridad deberán ser revisadas al menos dos veces por año.
- Todo el personal y proveedores de servicios de selección de personal que tengan contacto con datos personales, deberán firmar acuerdos de confidencialidad.
- Establecer protocolos de seguridad con proveedores de servicios de selección de personal de manera previa a que tengan acceso a datos personales de los candidatos.
- Revisión de los avisos de privacidad y políticas de proveedores relacionadas al tratamiento de datos personales.
- Determinar roles y responsabilidades claras para cada posición involucrada con el tratamiento de datos personales durante el proceso de selección.
- Capacitación al personal para identificar datos personales y su manejo adecuado.
- Establecer en los contratos con proveedores los estándares mínimos de seguridad que deberán adoptar para el tratamiento de datos personales.
- Evitar actividades que comprometan la divulgación o uso no autorizado de los datos personales.
- Establecer proceso disciplinario formal para empleados que vulneren las medidas de seguridad y/o hagan mal uso de datos personales.
- Auditar de manera regular los servicios, reportes y registros de proveedores para verificar que cumplen con un tratamiento adecuado de los datos personales de la organización y que cuentan con los estándares mínimos de seguridad requeridos.
- Establecer procedimientos y responsabilidades en caso de vulneraciones a las medidas de seguridad para evitar el mal uso de datos personales.
- Acceso a los datos personales previo registro con nombre de usuario y contraseña.

- Instalar antivirus en dispositivos de acceso y servidores.
- Habilitar bloqueos automáticos por inactividad en dispositivos de acceso.
- Controlar la instalación de *software* en los dispositivos de acceso. Inhabilitar instalaciones por los usuarios.
- Realizarse de manera periódica copias de respaldo con los datos personales.

b) Riesgo nivel 3. Las recomendaciones del nivel 2 más las siguientes:

- Habilitar sistema de monitoreo o accesos controlados a los datos personales.
- Establecer registro de usuarios con acceso a los datos personales.
- Revisión mensual de sistemas y bases de datos para verificar estado de las medidas de seguridad.
- Implementar bitácora de acceso y modificación de los datos personales.
- Recolección de evidencias en caso de vulneraciones a la seguridad y/o se presuma el tratamiento inadecuado de datos personales.
- Habilitar bloqueos o filtros de contenido para correo electrónico, internet y mensajería instantánea en los dispositivos de acceso.

Conclusiones

Conclusiones

El Derecho a la Intimidad se integra por el derecho a no ser molestado y el derecho a la autodeterminación informativa, siendo este último al que le corresponde proteger el tratamiento de los datos personales, los cuales consisten en la información que hace identificable a un individuo.

Los datos personales patrimoniales o financieros y sensibles requieren mayor protección debido a que existe mayor exposición de la integridad del titular.

Se entenderá como tratamiento a la obtención, acceso, manejo, aprovechamiento, remisión, transferencia, disposición, divulgación y almacenamiento de datos personales, en el que podrán intervenir el titular, responsable, encargados y terceros.

Las unidades económicas de prestación de servicios y producción de bienes durante su operación, llevan a cabo el tratamiento de datos personales y deberán contar con asesoría jurídica que evite infringir la normativa para la protección de los mismos, por lo que el departamento jurídico de la empresa deberá ser el modelo del manejo adecuado de datos personales.

Para que la gestión de datos personales sea correcta, los abogados pueden apoyarse de herramientas tecnológicas que permitan automatizar procesos y mejorar las operaciones.

La herramienta base para asegurar el tratamiento correcto de datos personales es la implementación del uso de la nube en cualquiera de sus tres modalidades (pública, privada o mixta).

Operar desde la nube facilita el trabajo en equipo, la supervisión de actividades y agrega controles que en un entorno físico o local no es posible utilizar, tales como control de accesos, envío de información cifrada y condicionantes para continuar el proceso operativo.

Dependiendo los recursos, volumen y especialización de las actividades del departamento jurídico de empresa, se determinará el tipo de nube que se ajuste al presupuesto y necesidades, por lo que es fundamental que se realice un análisis a detalle de los procesos, riesgos y requerimientos con la finalidad de disminuir las

desventajas del uso de cada tipo de nube para que ésta se convierta en una herramienta de vigilancia para el tratamiento de datos personales.

En particular, por lo que hace a la implementación de la nube en la contratación de personal, es posible llevar a cabo la gestión adecuada de datos personales en cualquiera de los tres tipos de nube, incluso en el tratamiento de datos patrimoniales y sensibles.

Durante el proceso de contratación de personal los datos involucrados pueden alcanzar hasta un nivel tres en riesgo por tipo de dato, por lo que se deberán tomar las medidas de seguridad necesarias para evitar cualquier contingencia y de ser posible, contratar servicios de terceros que validen perfiles de candidatos para que prescindir del tratamiento de datos personales sensibles y/o patrimoniales o financieros.

Cualquier modelo exitoso de implementación de nube que cumpla con las normativas en datos personales deberá involucrar procesos claros y eficientes, capacitación de los usuarios para concientizarlos respecto a los alcances de los datos personales y el uso de aplicaciones acordes a la operación que cuenten con medidas de seguridad acordes al riesgo de los datos personales que sean objeto de tratamiento.

Bibliografía

- CELIS, Marcos, “La Protección de la Intimidad como Derecho Fundamental de los Mexicanos”, *Estudios en Homenaje a Marcia Muñoz de Alba Medrano*, México, UNAM, 2006.
- FUNDACIÓN DE LA INNOVACIÓN BANKINTER, *Cloud Computing – La tercera ola de las tecnologías de la Información*, España, Fundación de la Innovación Bankinter, 2010.
- GARCÍA, Diego, “Derecho a la Privacidad”, *Derechos Humanos en la Constitución: Comentarios de Jurisprudencia Constitucional e Interamericana,* México, Suprema Corte de Justicia de la Nación, 2013.
- IDG COMMUNICATIONS, *Libro blanco “Hablando Cloud”, el punto de referencia sobre el Cloud Computing y la nube privada*, España, Microsoft, 2012.
- JOYANES, Luis, *Computación en la nube. Estrategias de Cloud Computing en las Empresas*, México, Alfa omega, 2012.
- MUÑOZ DE ALBA, Marcia, “Habeas Data”, *Estudios en Homenaje a Marcia Muñoz de Alba Medrano*, México, UNAM, 2006.
- OBSERVATORIO NACIONAL DE LAS TELECOMUNICACIONES, *Cloud Computing: Retos y Oportunidades*, España, Ministerio de Industria, Energía y Turismo del Gobierno de España, España, 2012.
- TÉLLEZ, Julio, *Lex cloud computing. Estudio jurídico del cómputo en la nube de México*, Instituto de Investigaciones Jurídicas, México, UNAM, 2013.
- TORRES Jordi, *Empresas en la nube. Ventajas y retos del Cloud Computing*, España, Ed. Libros de Cabecera, 2014.

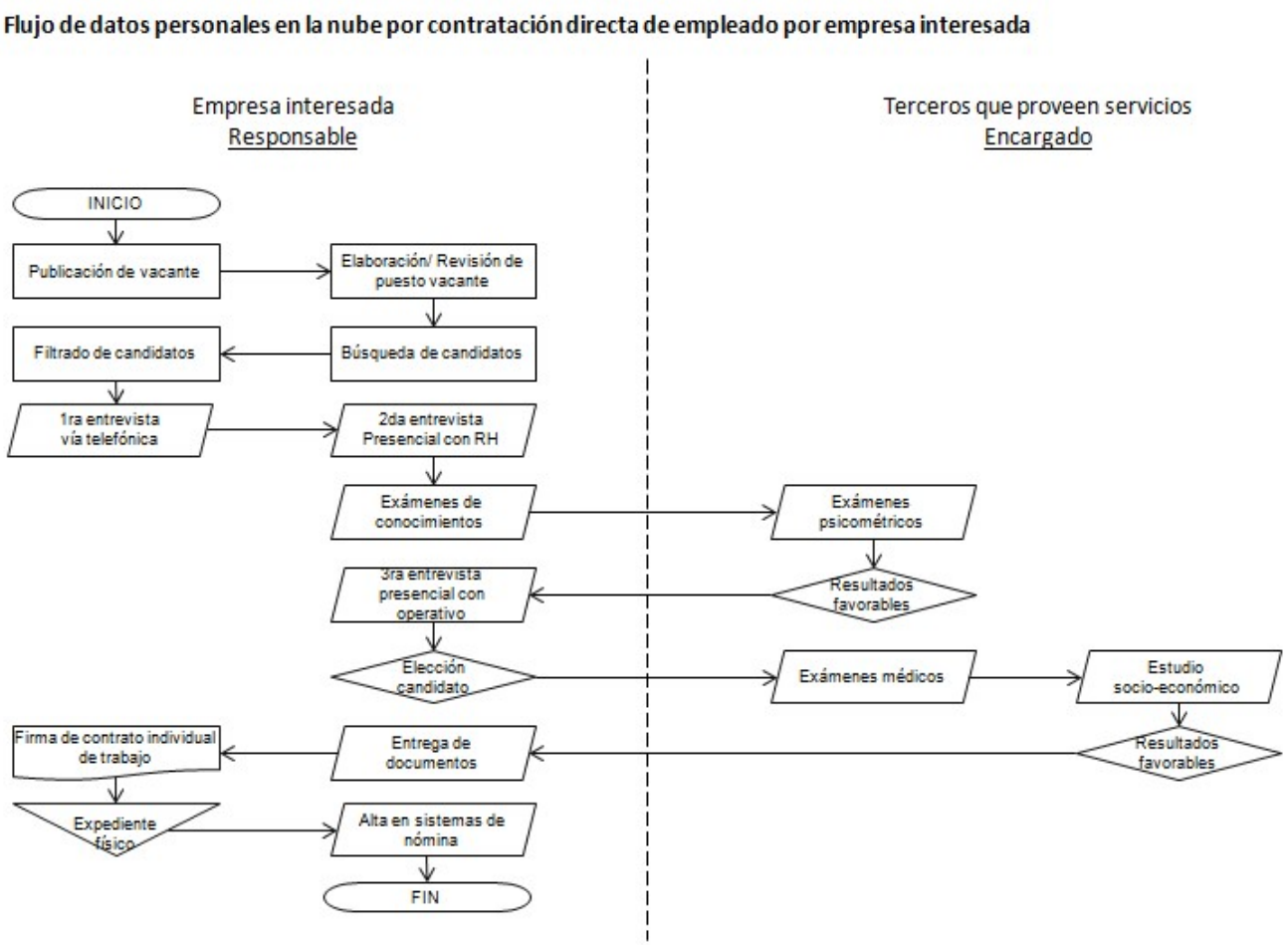
Artículos de revista

- DEL VECCHIO, José et al., “La computación en la nube: un modelo para el desarrollo de las empresas”, *Prospect,* Colombia, vol. 13 no. 2, 2015, pp. 81-87.
- HIPERTEXTUAL, “Cómo mejorar la seguridad de tus archivos en la nube”, España, 2014. *http://hipertextual.com/archivo/2014/09/seguridad-nube/*
- MELL Peter, et al. “The NIST Definition of Cloud Computing”, *NIST Special Publication*, Estados Unidos de América, número 800-145, septiembre 2011.
- PUCCINELLI, Oscar, “Evolución histórica y análisis de las diversas especies, subespecies, tipos y subtipos de habeas data en América Latina. Un intento clasificador con fines didácticos”. *Vniversitas*, Colombia, número 107, 2004.
- WARREN, Samuel y BRANDEIS Louis, “The Right to Privacy”, *Harvard Law Review*, Estados Unidos de América, Vol. IV No. 5, diciembre 1890.

Anexos

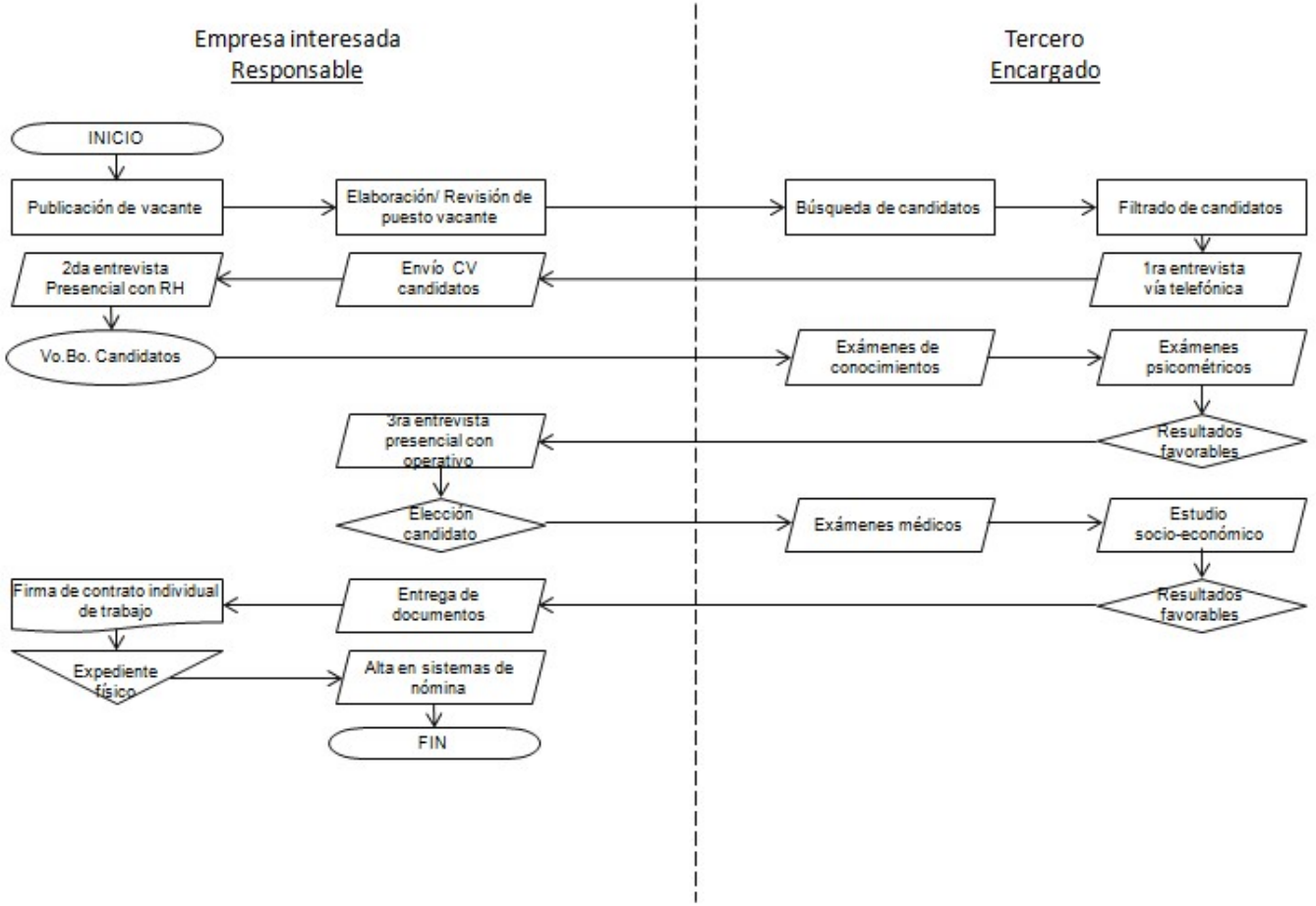
Anexos

Anexo I



Anexo II

Flujo de datos personales en la nube por contratación de empleado con selección a través de tercero



Anexo III

Flujo de datos personales en la nube por contratación de empleado a través de tercero