### ***Amenazas y riesgos***

Procedemos a hablar ahora acerca de las amenazas y de los riesgos más destacables que se nos pueden llegar a presentar ante el uso de *Cloud Computing* y además veremos cómo podemos hacerles frente ante situaciones de peligro más comunes.

Cuando decidimos hacer uso de uno de los modelos de contratación o de despliegue en la nube, recae sobre nosotros la duda sobre cuál de estos tipos sería el más conveniente para garantizar la seguridad de nuestros datos. Es entendible que la seguridad de las aplicaciones virtuales en la nube requiere realizar tareas mucho más complejas que la seguridad de las aplicaciones de escritorio que teneos instaladas en nuestros ordenadores o dispositivos electrónicos. Es cierto que los proveedores han de garantizar un plan de privacidad que proteja de forma permanente sus servidores de centros de datos y por tanto de mantenerlos actualizados constantemente.

Pero el proveedor no tiene por qué encargarse de todo el tema de la privacidad, sino que también las propias organizaciones han de encargarse de dirigir particularmente el tema de la seguridad por medio de su equipo o departamento de sistemas que actualice a las últimas versiones y emplee medidas de seguridad acertadas ante cualquier acción que ponga en peligro la confidencialidad de los datos. Entre estas acciones tan temidas nos encontramos con los conocidos ataques de ciberseguridad o ataques *hackers* que podemos contenerlos por medio de sistemas antivirus, realizando copias de seguridad, controlar qué usuarios son los que se registran y acceden a las aplicaciones, actualizaciones diarias o frecuentes, etc. [16]

Tanto el proveedor como los usuarios tiene parte de responsabilidad con las diferentes tareas de seguridad, mientras que el proveedor normalmente se encarga de aquellas incidencias relacionadas con la electrónica como comprobar el correcto funcionamiento de los servidores en los centros de datos, el usuario ha de hacerse cargo de todas aquellas tareas que ya hemos mencionado anteriormente para que su sistema particular no sea víctima de los prejuicios de ataque informáticos. Por tanto, para que los requisitos de seguridad necesarios queden claro de quién ha de hacer cada parte, el proveedor y el usuario firman un contrato llamado **ANS** o **Acuerdo de Nivel de Servicio** donde se especifican los puntos que han de cumplirse con motivos de seguridad para los servicios demandados por los usuarios y así quede constancia de la responsabilidad que recae sobre cada una de las partes. Es muy importante que antes de firmar cualquier acuerdo, los usuarios decidan qué modelo de despliegue o de contratación van a seleccionar de cara al presupuesto de seguridad puesto que unos presentan aspectos diferentes de otros en función de las necesidades. [16]

Una vez dicho esto, vamos a ver algunos tipos de amenazas más frecuentes a las que los usuarios nos encontramos cuando utilizamos con poca vulnerabilidad las herramientas que nos ofrece la nube: [16] [28]

|  |  |  |
| --- | --- | --- |
| **Amenaza** | **Descripción** | **Prevención** |
| **Ataques de ciberseguridad (*hackers*)** | Personas que por medio de la red estafan y manipulan los datos de los clientes por medio de software envenenado, aplicaciones con *malware*, virus gusano o cualquiera de los métodos que ejerza. | Informar a los usuarios acerca del peligro que conlleva ciertas actividades cibernéticas y cómo poder solventarlas y mejor aún, prevenirlas. |
| **Interfaces poco fiables** | Aquellas interfaces sobre todo de registro que carecen de seguridad pueden poner en peligro la privacidad de los usuarios. | Sistema de autenticación fiable con cifrado.  Solventar incidencias de seguridad. |
| **Amenazas internas** | Los propios trabajadores de la nube pueden suponer una amenaza ante cualquier fallo de privacidad cometido ya sea accidental como voluntariamente. | Contratos con cláusulas legales sobre la privacidad de los datos de los clientes. |
| **Compartición de tecnologías** | Si nuestra empresa tiene contratado un servicio en a la nube pública donde compartimos aplicaciones con el resto de las empresas, un error nuestro o de cualquiera de ellas puede provocar fallos en los servidores globales y afectar a todas las organizaciones involucradas. | Manuales bien definidos sobre la instalación y mantenimiento del software de gestión.  Indicar los fallos propagados por medio de trazas de log. |
| **Pérdida de información** | Los usuarios más vulnerables pueden caer en manos de hackers aportando información confidencial por medio de un *malware* desarrollado por ellos o incluso pérdidas de datos por transferencias incontroladas. | Asegurar la vía de comunicación de los trámites con buenos métodos de cifrado.  Informar a los usuarios acerca de los métodos cibercriminales más peligrosos.  Mecanismos de protección de claves. |
| **Suplantación de identidad** | Los cibercriminales pueden conseguir las credenciales de acceso de los usuarios para manipularla o falsificar datos. | No permitir traspasar las claves entre los usuarios por ningún medio.  Inicios de sesión monitorizadas. |
| **Desconocimiento de seguridad** | Falta de conocimiento de los responsables que ejercen las pautas de seguridad de la organización y da lugar a brecha de seguridad peligrosas. | Monitorizar toda la información relevante para el caso incluidas las trazas de los logs. |

Tabla 4 – Amenazas de Cloud Computing

Compaginado con las amenazas, hablaremos acerca de los riesgos que puede tomar el uso de los servicios en la nube junto con sus debidas precauciones, ya que una amenaza puede llegar a provocar graves consecuencias para la seguridad de la información: [16] [28]

|  |  |  |
| --- | --- | --- |
| **Riesgo** | **Descripción** | **Prevención** |
| **Usuarios con privilegios** | Es necesario tener un determinado control sobre todos aquellos usuarios con privilegios (superadministradores) para que no se consientan acciones tanto involuntarias como con dolo hacia los clientes que alteren la privacidad de sus datos. | Tomar la sabia decisión sobre quién debe tener determinados privilegios de acceso a la información más vulnerable. |
| **No cumplir con las normas** | Si el proveedor de servicios no cumple con la normativa legal sobre los derechos de los usuarios pueden tener consecuencias penales y administrativas ante la ley. | Implantación de auditorías para controlar la normativa legal de la empresa del proveedor. |
| **Ubicación de los datos** | Es muy probable que los datos de los clientes que ofrecen por el uso de los servicios en la nube sean administrados por entidades de gestión de datos fuera de su país de residencia. Lo que puede provocar cierta controversia normativa entre el choque de distintas legislaciones entre estos países. | Consultar cuales son las normas que ejercen la ley atendiendo al lugar de residencia del proveedor y del usuario en función del caso que se presente. |
| **Datos aislados** | En caso de que los datos sean compartidos en infraestructura de una empresa con otra, hay que ceñirse de que esos datos puede que no estén bien cuidados y protegidos por posibles intermediarios sin derechos. | Cubrir todo tipo de medida de privacidad para que los datos se mantengan seguros tras su tratamiento entre distintas entidades. Por ejemplo, utilizando técnicas de cifrado sofisticadas. |
| **Recuperación y restauración** | Si una empresa sufre cualquier tipo de incidente grave que no permita salvar los datos que tratan a tiempo, puede tener graves consecuencias ante la ley por parte de los clientes. | Adoptar sistemas de prevención de pérdida de datos, cuentas de recuperación, realizar copias de seguridad frecuentemente, etc. |
| **Soporte de investigación** | Lamentablemente los proveedores no suelen optar por un plan de investigación que ayude a vigilar los datos de los usuarios en caso de cualquier incidente que pueda llegar a afectarles. | Aumentar los logs sobre la visualización de los datos de los usuarios, duplicar los datos en cualquier servidor externo, … |
| **Viabilidad a largo plazo** | Existen casos en los que el proveedor de los servicios cambia por otro y por tanto la normativa legal sobre privacidad que ejercía uno no tiene por qué impartirla el otro. | Asegurar e informar a los clientes que sus datos pueden ser accedidos por ellos y no sufren modificaciones indeseadas sin su consentimiento. |

Tabla 5 – Riesgos de Cloud Computing

Hasta aquí abarcamos la primera parte de este capítulo como base preliminar al contenido del desarrollo del trabajo conociendo pues los conceptos generales de la computación en la nube que nos ayudarán a enlazarlos con los próximos capítulos. A partir de ahora nos iremos acercando al estudio de los objetivos de nuestro trabajo, primero haremos una visión general sobre *Amazon Web Services (AWS)*, de sus características y sus servicios en la nube de donde extraeremos los datos necesarios con los que posteriormente trabajaremos y aplicaremos los algoritmos propuestos para evaluar finalmente los resultados.