

Gobernanza en la nube



Aviña Pérez José

3-A 301 CDIA

Actividad 4

Índice

Introducción…………………………………………………………………………………………..pag3

Cumplimiento de normativa de la nube……………………………………………….pag4

Gobernanza en la nube…………………………………………………………………………pag5

Leyes y regulaciones…………………………………………………………………………….pag6

Contratos………………………………………………………………………………………….…..pag7

Estándares…………………………………………………………………………………………...pag8

Auditorías……………………………………………………………………………………………..pag9

Informes de la auditoría……………………………………………………………………….pag10

Conclusión…………………………………………………………………………………………….pag11

Glosario…………………………………………………………………………………………………pag12

Introducción

Todos sabemos lo que son las leyes, la nube y los contratos, pero no el cómo van relacionadas una de la otra, la nube ya es algo cotidiano en nuestra vida diaria, al utilizar un banco ya estamos utilizando la nube por lo que es necesario conocer las leyes que giran en torno a esta.

Una vez que una empresa está en la nube, debería preocuparse acerca de cómo el proveedor de nube le ayudará a mantener el cumplimiento con las leyes, como el Reglamento General de Protección de Datos (GDPR) de Europa o la HIPAA en EE. UU. Este debate no debe comenzar una vez que el servicio en la nube se haya establecido, sino que se debe plantear desde el mismo inicio de los análisis. A menudo, las empresas se encuentran en la nube mucho antes de lo que lo planearon y esto complica las cosas. Uno de los principales retos de la nube es aquel que permita una interfaz de autoservicio para que facilite la configuración, cambio y salida del cliente de los servicios en la nube. Sin embargo, lo que no está claro es quién será el encargado, por parte del cliente, de realizar esto. Hoy en día, podría ser cualquier persona. Todo lo necesario es una tarjeta de crédito corporativa y un departamento puede comenzar por su cuenta a colocar los datos en la nube. El término para esto no es nuevo, se trata de «TI en la sombra». Este término está muy de moda últimamente debido a las características de la nube.

El mantener las leyes de la nube es muy complicado y mas para las empresas ya que estas requieren una interfaz de autoservicio, aunque ese tipo de servicio sea esencial y muy útil para la empresa también hay riesgos como que cualquier persona puede disponer de este tipo de servicios sin darles el fin establecido.

Cumplimiento de normativa de la nube

Gobernanza en la nube

La gobernanza es la supervisión que llevan a cabo los altos ejecutivos y la junta directiva sobre la empresa. La gobernanza en la nube es una extensión de dicha supervisión en la nube. La gobernanza es fundamental. Sin ella habría demasiadas preguntas sin resolver acerca de las metas y los objetivos de la empresa que harían la gestión de la nube y su seguridad sumamente difíciles. Antes de que una empresa llegue a la nube, deberían definirse sus metas y objetivos. Ambos deberían guiarse por las leyes, regulaciones y contratos aplicables. Más allá de los aspectos legales, la gobernanza en la nube dirige a los empleados por el camino correcto con el fin de ayudar a la empresa a alcanzar sus metas y objetivos. Los errores graves pueden hacer que la nube termine complicando las cosas, haciendo que los usuarios no puedan realizar su trabajo. Los errores incluso podrían llevar la empresa a los tribunales. La junta directiva y los ejecutivos a cargo de la gestión de la empresa deben tener prestar atención y cuidado a la nube.

La Gobernanza en la nube es la supervisión sobre la empresa, esta dicta las metas a alcanzar y los objetivos, esto sirve para dirigir a los empleados a un correcto desempeño, de no ser acatos estos objetivos podría haber consecuencias jurídicas.

El primer punto de cualquier debate de cumplimiento de normativa es la ley. Las empresas y sus abogados deben definir qué leyes se deben seguir. También deberían ser claros respecto a las consecuencias de su incumplimiento. Una vez que se identifiquen las leyes, es importante preguntarse qué controles de seguridad se deben implantar con el fin de cumplir con las leyes y regulaciones aplicables. Las regulaciones con el GDPR de la UE requieren un gran trabajo de seguridad respecto a la información personal. El GDPR de la UE tiene restricciones muy específicas respecto a dónde se pueden procesar y almacenar los datos bajo el ámbito de dicha regulación. Esto conduce a un posible problema con la nube debido al funcionamiento de la misma. Sin embargo, se pueden adoptar controles con la mayoría de los proveedores de nube para cumplir con los requisitos del GDPR de la UE.

Cada empresa define sus leyes, su cumplimiento y que pasa si se incumple alguna de las mismas, la empresa debe adaptarse y buscar cumplir con todos los requisitos del GDPR.

Leyes y regulaciones

Contratos

Los contratos definen un acuerdo formal entre dos o más partes. Cuando una empresa celebra un contrato, está obligada a estar a la altura de sus términos. Su incumplimiento podría suponer graves sanciones económicas. Es muy probable que una organización que procesa o almacena información de tarjetas de crédito tenga un acuerdo con empresas de tarjetas de crédito que les obliguen a implementar elementos específicos del Payment Card Industry Data Security Standard (PCIDSS). Para procesar tarjetas de crédito, una empresa firma un acuerdo mediante el que se compromete a cumplir con los 12 requisitos de seguridad del estándar. El nivel en el que se deben implementar los requisitos depende del número de transacciones procesadas al año. Asimismo, una empresa también debería analizar si alguno de sus contratos con sus clientes estipula lo que puede o no realizar con la nube. ¿Hay alguna repercusión en el cumplimiento de normativa si utiliza una nube de algún tipo, como pública, privada, comunitaria, etc.?

Los acuerdos son muy importantes en una empresa ya que se definen los términos y condiciones, el incumplimiento de este puede llevar alguna sanción económica, en el contrato se estipula el control que llevara la empresa sobre la tarjeta.

Estándares

Numerosas empresas utilizan estándares como los ISO 27001 o NIST SP 800-53 como base para la implementación de controles de seguridad. Si una empresa ha decidido utilizar la ISO 27001 como su estándar, debe formar a sus empleados para que se implementen los controles adecuados. Esto se amplía a la nube. De hecho, ISO ha aislado los controles específicos para la nube y los ha abordado en la ISO 27017.

Los controles de seguridad de las empresas se hacen a partir de ciertos estándares como ISO 27001 o NIST SP 800-53, la empresa esta obligada a capacitar a sus empleados sobre este.

Una forma de evaluar el nivel de cumplimiento de las leyes, regulaciones y contratos es realizar una auditoría. Las auditorías pueden ser internas o externas. Una auditoría interna, llevada a cabo por auditores de la propia empresa, proporciona una autoevaluación para determinar su nivel de cumplimiento. Sin embargo, los resultados de una auditoría interna se pueden llegar a considerar como sesgados dado que los auditores podrían considerarse parciales en sus conclusiones. Para proporcionar una opinión más objetiva, es posible elegir una empresa de auditorías externa e independiente para que realice una auditoría de la compañía. Las auditorías que analizamos aquí respecto a la nube son aquellas realizadas por el proveedor de nube. La mayoría de los proveedores de nube no verían con buenos ojos que clientes de sus datacenters realicen su propia auditoría, por lo que nos basaremos en auditorías realizadas por empresas externas e independientes.

Las auditorias son la mejor forma de evaluar el cumplimiento de las leyes, siempre es mejor contratar a una auditoria independiente esto para tener mejores resultados y una mejor imagen.

Auditorías

El resultado de una auditoría se encuentra en el informe de la misma. Los informes están estandarizados por el American Institute of Certified Public Accountants (AICPA). Todas las empresas deberían solicitar el informe de auditoría SOC 2®. El informe SOC 2® está destinado para las organizaciones de servicio, como los proveedores de nube. Muestra el cumplimiento con los controles definidos en la ISO 27001 o en el Marco de ciberseguridad (CSF) del NIST, por ejemplo. Los controles se evalúan frente a los cinco criterios de servicios de confianza del AICPA, que son:

• Seguridad

• Disponibilidad

• Confidencialidad

• Integridad en el procesamiento

• Privacidad

Estos informes podrían ser de tipo 1 o de tipo 2. Un informe de tipo 1 muestra el estado de los controles en un momento específico y que los mismos están diseñados e instalados en un nivel de adecuación. Un informe de tipo 2 muestra la efectividad operativa de los controles a lo largo de un periodo de tiempo, por ejemplo, de seis meses. Un cliente de nube debería solicitar estos informes, pero es posible que el proveedor de nube no esté dispuesto a proporcionarlos debido a que pueden contener información confidencial sobre sus actividades. Otra opción es un SOC 3®, destinado como un informe de uso general. Contiene muy poca información respecto a la actividad del proveedor de nube. Sin embargo, proporciona eficazmente al cliente el sello de aprobación (o no) del proveedor de nube por parte del auditor.

Existen 2 tipos de resultados de las auditorias, están el tipo 1 que muestra el estado de los controles, el tipo 2 muestra la efectividad operativa, aunque también existe un tipo de informe general con muy poca información, el resultado se encuentra en el informe de la misma.

Informes de la auditoría

Conclusión

Las leyes de la nube son de suma importancia, con ellas todo fluye de manera concisa y ordenada, permite un mejor manejo del rendimiento y permite imponer una sanción si hay algún incumplimiento de alguna de las mismas, todas estas leyes llevan consentimiento por parte de la empresa y consumidor por lo cual son seguras y confiables.

Glosario

**Data centers:** Se denomina Centro de Proceso de Datos al espacio donde se concentran los recursos necesarios para el procesamiento de la información de una organización. También se conoce como centro de cómputo en Hispanoamérica y en España como centro de cálculo, centro de datos, centro de proceso de datos o centro de informática.

**Interfaz:** Una interfaz se utiliza en informática para nombrar a la conexión funcional entre dos sistemas, programas, dispositivos o componentes de cualquier tipo, que proporciona una comunicación de distintos niveles, permitiendo el intercambio de información. Esto es un ejemplo de la realidad virtual.

**Auditorías:** Inspección o verificación de la contabilidad de una empresa o una entidad, realizada por un auditor con el fin de comprobar si sus cuentas reflejan el patrimonio, la situación financiera y los resultados obtenidos por dicha empresa o entidad en un determinado ejercicio.

**Adecuación:** La adecuación es la propiedad de los textos basada en el cumplimiento de ciertas normas y principios relacionados con el emisor, receptor, el tema y la situación, y que afecta a la estructura, pertinencia y comprensibilidad de un texto.