Cloud Computing, controles

En el post anterior recorrimos las **diferentes tipos de riesgos** que presenta el Cloud Computing y terminamos diciendo que es **necesario utilizar los controles adecuados** para poder mitigarlos. Y estos controles, comentamos que los íbamos a encontrar en **marcos de trabajo**. Pues bien, dedicaremos este post a explicar lo que son los controles y qué debe hacer un auditor para asegurarlos. Asimismo, y a modo de ejemplo, estudiaremos una serie de controles que responden a riesgos concretos que he extraído de diferentes fuentes. Sin más dilación, comenzamos.

¿Qué es un control? En pocas palabras, podríamos decir que es un **mecanismo que define una organización con la finalidad de mitigar un riesgo**. Y con mitigar nos referimos a, por un lado, reducir la probabilidad de ocurrencia del riesgo y, por otro lado, reducir el daño que pueda causar en caso de que ocurra. Estos criterios, **probabilidad e impacto**, aunque no lo dijéramos en el anterior post explícitamente, suelen ser los dos ejes de análisis a la hora de priorizar los riesgos.

Para entenderlo mejor, pongamos un ejemplo. Si tenemos un riesgo concreto de privacidad y seguridad (tal y como vimos en el anterior post) con los datos que almacenamos en la nube, póngase, riesgo de que nuestros datos sean interceptados por terceros no autorizados en la red de comunicaciones que mantenemos con el proveedor, podríamos tener el siguiente control: asegurar que los datos en tránsito por las redes de comunicación oportunas entre proveedor y consumidor están encriptados con claves privadas que solo conoce el segundo [1]. Esto es, si cumplimos con lo que dice el control, logramos mitigar el riesgo.

¿Fácil? Pues en realidad es más complejo de lo que parece. En primer lugar, existen multitud de riesgos concretos que debemos tener en cuenta, y es por eso, que como decíamos en el

anterior post, vamos a necesitar guías y marcos de trabajo que nos permitan considerarlos sin que se nos escape ninguno. Y además, y esto aún no lo he dicho, **los controles no solo deben implementarse… Deben auditarse**. En otras palabras, debe asegurarse que los controles se cumplen. Y para ello, lo normal es que cuando se define un control, se le asocien una serie de pruebas de control o acciones de auditoría.

Para ese mismo ejemplo que veíamos antes, recogido de un documento oficial de ISACA [1], se definen las siguientes acciones de auditoría: (1) obtener las políticas de encriptación y procedimientos para datos en tránsito de la organización, (2) evaluar si los procedimientos incluyen lo siguiente: clasificación de datos en función de la sensibilidad (top secret, confidential, company confidential, public), tecnologías de encriptación adecuadas, gestión de claves apropiada y una lista de organizaciones externas del consumidor que poseen las claves de desencriptado. ¿Ya es algo más concreto verdad? Parece que empezamos a tener el control, valga la redundancia, sobre el control que hemos definido para el riesgo que queremos mitigar.

Dicho esto, y ahora que entendemos lo que es un control y cómo se debe asegurar, he tratado de identificar ciertos riesgos concretos para nuestro paradigma, el Cloud Computing, con el objetivo de haceros ver algunos controles que nos pueden ayudar a mitigarlos. Con esa finalidad, he construido una **tabla con tres columnas**: dominio (tipo de área donde se enmarca el control), control (definición del control, lo que se debe hacer) y riesgo mitigado (problema al que responde el control).

Para construir dicha tabla, me he apoyado principalmente en el documento [1], el cual define una serie de controles para la mitigación de riesgos en el Cloud Computing haciendo uso del marco de trabajo **COBIT** y el marco de trabajo **COSO ERM**. Mi trabajo ha consistido en agrupar los controles más significativos, descartar aquellos redundantes, resumirlos,

clasificarlos por dominios y relacionarlos con el riesgo que buscan mitigar. Además, he usado a modo complementario los documentos [2] [3] [4] y he considerado los contenidos del anterior post para la definición de los riesgos mitigados. La tabla es la siguiente:

Dominio	Control	Riesgo mitigado
Gestión de identidades y accesos.	**Asegurar** una **asignación y designación de identidades** en las aplicaciones alojadas en la nube de la organización **controlada y alineada con las políticas internas** de gestión de usuarios.	Acceso no autorizado a recursos y datos.
	Asegurar que la **responsabilidad de la autenticación de usuarios pertenece al consumidor** del servicio y que se usan **tecnologías single sign-on y OpenID** para todos los servicios consumidos.	Acceso no autorizado a recursos y datos.
Seguridad e integridad de datos.	**Encriptar los datos en tránsito** por las redes de comunicación oportunas entre proveedor y consumidor con claves privadas que solo conoce el segundo. Uso de una **VPN** apropiada.	Revelación y pérdida de datos.
	Encriptar los datos contenidos en las bases de datos y sistemas del proveedor con claves que solo conozca el consumidor.	Revelación y pérdida de datos.
	Encriptar los datos de las copias de seguridad de las bases de datos y sistemas del proveedor.	Revelación y pérdida de datos.
	Confirmar que los **datos de prueba (testing) no contienen información confidencial o sensible**, y que no se usan datos históricos del sistema de producción para testear aplicaciones alojadas en la nube.	Revelación de datos.
	Asegurar que las **claves de encriptado** están **protegidas adecuadamente** ante accesos no autorizados, que existe una **segregación de deberes** entre los gestores de las claves y los usuarios a través de una **política de gestión de claves** y que las claves tienen **copias de seguridad**.	Revelación y pérdida de datos.
Portabilidad e interoperabilidad.	**Asegurar** que los **procedimientos, capacidades** y **alternativas** para **migrar las operaciones en la nube a otro proveedor están** previamente **definidas** al consumo del servicio en caso de que sea necesario por incumplimiento de los requisitos contractuales o cese del servicio del proveedor contratado.	Impacto en la continuidad de negocio. Interrupción de los servicios prestados.
Seguridad de sistemas e infraestructuras.	**Asegurar** que los **sistemas** están **aislados y protegidos** por controles de seguridad a través de **herramientas de virtualización** para prevenir accesos no autorizados y ataques.	Indisponibilidad de sistemas y revelación de datos.

	Confirmar que el **diseño** de las aplicaciones alojadas en la nube incluye **aspectos de seguridad a nivel de arquitectura** aprobados por expertos y que dicho diseño hace hincapié en las **interdependencias con otros sistemas** y aplicaciones.	Indisponibilidad de sistemas.
	Confirmar que todas las **herramientas** utilizadas en el **desarrollo, gestión y monitorización** de las aplicaciones están **documentadas, aprobadas y analizadas** en función del efecto que puedan causar en los controles de seguridad establecidos.	Indisponibilidad de sistemas y revelación de datos.
Contratos.	**Asegurar** que el **equipo legal del consumidor ha identificado y comunicado** al proveedor los **requisitos contractuales** oportunos, y que este último, ha aceptado cumplirlos.	Incumplimiento de obligaciones contractuales.
	Confirmar que el **consumidor realiza una monitorización** constante para confirmar que **se cumplen** las **obligaciones reflejadas en el contrato** con el proveedor.	Incumplimiento de obligaciones contractuales.
Cumplimiento.	**Asegurar** que los aspectos legales relativos a **requisitos funcionales, jurisdiccionales o contractuales son considerados por ambas partes, proveedor** y **consumidor**, estando todos ellos documentados, aprobados y monitorizados.	Incumplimiento normativo.
	Confirmar que todas las **regulaciones** sobre **protección de datos** que afectan a las actividades de la compañía están **identificadas, clasificadas y documentadas**. **Asegurar** que la **plataforma** de Cloud Computing contratada **no incumple ninguno de los requisitos u obligaciones** contempladas en dichas regulaciones.	Incumplimiento normativo.
	Asegurar que las **responsabilidades de protección de datos están correctamente definidas y repartidas** entre proveedor y consumidor en función del modelo de despliegue elegido.	Incumplimiento normativo.
	Asegurar que el **proveedor** ofrece garantías de seguridad a través de la **certificación ISO 27001**.	Incumplimiento normativo.

Tabla. Controles y riesgos mitigados Cloud Computing.

Espero que esta tabla os haya servido para haceros una idea de qué controles necesitamos si nuestra compañía quiere adoptar el Cloud. Supongo que os habréis dado cuenta, que tal y como adelantamos en el anterior post, todo gira entorno a controlar la **complejidad del paradigma** y asegurar que trabajamos con un **tercero que** nos **ofrece** las **garantías** necesarias. Asimismo, comentaros que si os quedáis con la curiosidad y queréis ver qué acciones de auditoría concretas tiene asociadas cada control, os recomiendo acudir al documento [1].

Para finalizar, como reflexión, permitidme deciros que si os fijáis, existen muchos tipos de controles, algunos más técnicos y otros quizás más de gestión. Y que a veces, al menos yo (como estudiante de ingeniería) y con ciertas preferencias personales hacia el mundo del desarrollo, nos cegamos con los aspectos tecnológicos y no somos capaces de ver lo importantes que son los aspectos organizativos. Si no hay una política de gestión de claves bien definida, da igual lo sofisticado o puntero que sea tu sistema criptológico, vas a tener vulnerabilidades. De la misma manera, por muy buena política de gestión de usuarios que hayas definido, como no uses una tecnología robusta que permita implementar de manera segura sus directrices, tienes un problema. Lo mismo, para los contratos y cumplimientos…

Con esto simplemente os quiero hacer ver que las TIC deben estar alineadas con negocio. Que las TIC, cada vez están más afianzadas como parte de la estrategia de la organización. Y que las TIC, cada vez están más lejos de ser una simple capa de soporte. En definitiva, quería remarcar que un **auditor TI** no es solo un profesional que asegura con su buen criterio que todo está en orden, sino también un **puente entre** el **negocio** y la **tecnología**.

Hasta aquí el cuarto post. ¡Gracias por leerme y nos vemos en el siguiente!

[1] «IT Control Objectives for Cloud Computing», ISACA, acceso el 16 de noviembre de 2019, https://www.isaca.org/chapters2/kampala/newsandannouncements/Documents/IT%20contro%20objectives%20for%20Cloud%20computing.pdf

[2] «Protiviti's View on Emerging Risks – Cloud Computing», KnowledgeLeader, acceso el 16 de noviembre de 2019, https://www.knowledgeleader.com/knowledgeleader/content.nsf/web+content/nlpreviewjuly2019

[3] Zacharias Enslin, «Cloud computing adoption: Control objectives for information and related technology (COBIT) – mapped risks and risk mitigating controls». African Journal of Business Management 6 37 (2012): 10185-10194, acceso el 16 de noviembre de 2019, https://oceano.biblioteca.deusto.es/permalink/f/193pu0n/TN_crossref10.5897/AJBM12.679, https://academicjournals.org/journal/AJBM/article-full-text-pdf/363FCF530555

[4] «Riesgos y amenazas en Cloud Computing», INTECO-CERT, acceso el 16 de noviembre de 2019, https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_riesgos_y_amenazas_en_cloud_computing.pdf