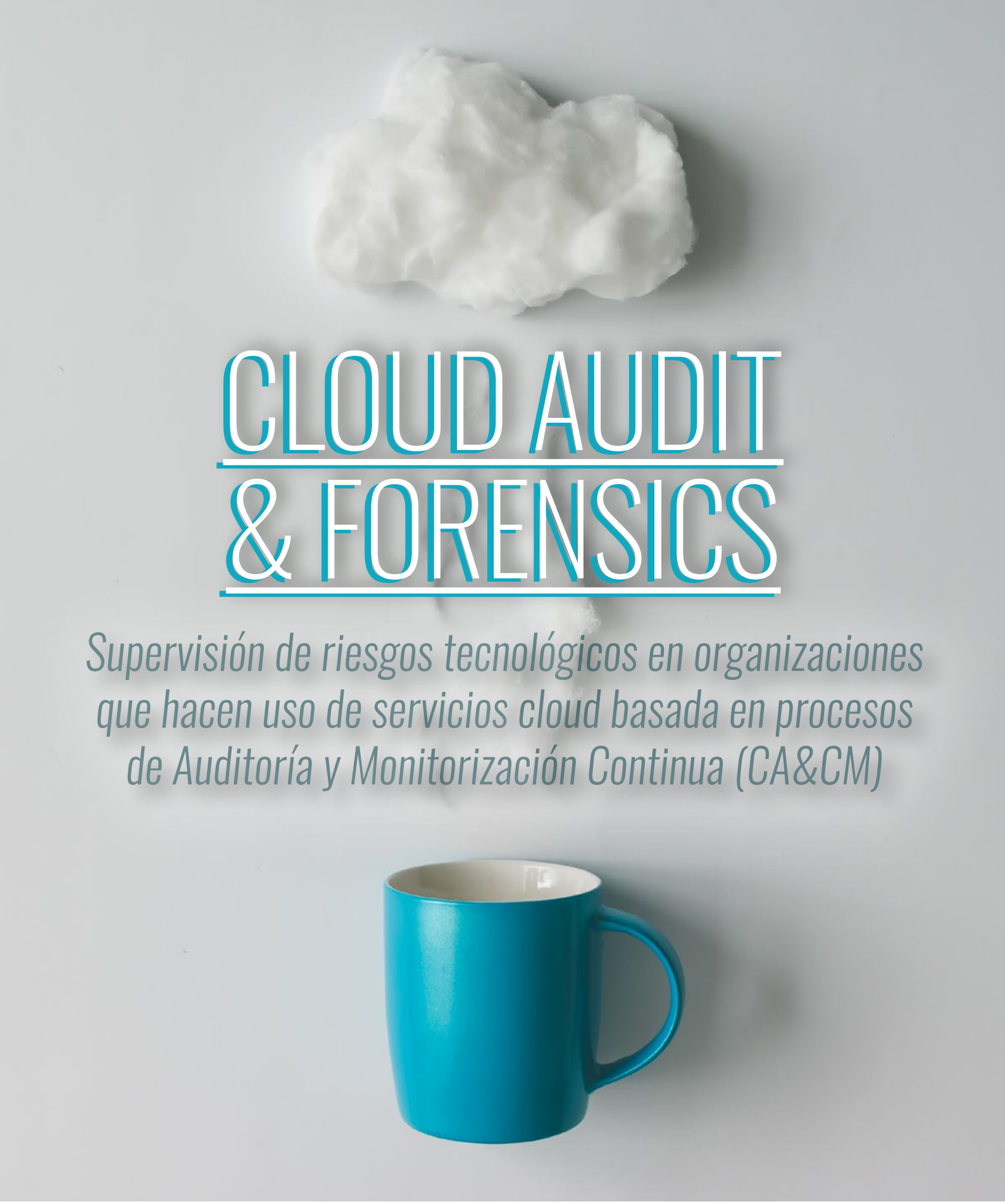


CLOUD AUDIT & FORENSICS

Supervisión de riesgos tecnológicos en organizaciones que hacen uso de servicios cloud basada en procesos de Auditoría y Monitorización Continua (CA&CM)

Una iniciativa de:

isms forum

CSA ES cloud security SPAIN alliance℠

Autor y coordinador

Pablo Castaño Delgado, Analista de Ciberseguridad (GRC), Banco Santander, y Miembro del Comité Técnico Operativo del Capítulo Español de Cloud Security Alliance. Anteriormente, Auditor interno de sistemas, Sareb.

CLOUD AUDIT & FORENSICS

Supervisión de riesgos tecnológicos en organizaciones que hacen uso de servicios cloud basada en procesos de Auditoría y Monitorización Continua (CA&CM)

ÍNDICE

1 INTRODUCCIÓN

El modelo de relación de las organizaciones con la tecnología ha ido evolucionando con el paso de los años, partiendo de una visión inicial en la que la tecnología era un bien más en el que invertir, pero sin mucho peso dentro de la organización; hasta llegar a una visión en la que la tecnología ya no solo es un recurso que aporte valor a negocio, sino que incluso ayuda a desarrollarlo, mediante la definición de nuevos modelos de negocio basados en la tecnología.

Otro componente fundamental para entender la evolución de la tecnología en la organización es el modo en el que ambas se relacionan. La adopción de un modelo que no se base en el despliegue de recursos tecnológicos dentro de los límites físicos del a organización es relativamente reciente. Sin embargo, en la actualidad, existen diversos modelos de gestión tecnológica que se extienden más allá de los límites de la organización, entre los que se encuentra la computación en la nube.

De entre todos los modelos de externalización de recursos tecnológicos, la computación en la nube ha sido uno de los más extendidos, con un incremento considerable desde que empezó a integrarse en entornos corporativos a finales de la década de los 90 y principios de los 2000. En la actualidad, esta tecnología ya no se considera una moda o una tecnología de vanguardia como ocurría hace años, sino que se ha convertido en un recurso tecnológico básico para un sinfín de organizaciones de tamaños y sectores heterogéneos.

La computación en la nube ofrece una facilidad de uso, configuración, gestión y mantenimiento que por lo general resultan mucho mayores a las de las tecnologías desplegadas on premise, con unos costes competitivos y la posibilidad de ajustar la capacidad de forma dinámica a medida que se producen fluctuaciones en la demanda. Esta mayor abstracción del servicio con respecto de los recursos tecnológicos subyacentes es aportada por el CSP (Cloud Service Provider), que pone a disposición de la organización tecnología en forma de servicios.

Considerando la importancia que ha adquirido la tecnología para las organizaciones, lograr una supervisión eficiente de ésta y una gestión efectiva de los riesgos a los que se ve expuesta resulta una necesidad más que una opción. Al mismo tiempo, la introducción de ecosistemas tecnológicos más complejos y descentralizados ha incrementado los retos a los que las organizaciones se enfrentan para lograr un nivel de aseguramiento adecuado.

Si bien desde un punto de vista funcional y operativo los servicios cloud ofrecen innumerables ventajas, la supervisión y control de éstos se vuelve mucho más compleja, y en ocasiones impracticable. Influyen en estas actividades factores que incrementan dicha complejidad, como la necesidad de coordinación con el CSP, cuya relación se define a nivel contractual; o la mayor opacidad y dificultad de acceso a las capas inferiores del modelo de arquitectura tecnológico utilizado para dar soporte a los servicios en la nube.

El presente documento aborda la problemática surgida de la necesidad de supervisión de los riesgos tecnológicos introducidos en las organizaciones como resultado de la adopción de servicios cloud, utilizando para ello un modelo de supervisión que se adapte a las necesidades y características de los servicios en la nube.

El enfoque utilizado para plantear la solución a dicha problemática se basa en tres pilares fundamentales: (i) el desarrollo de recursos suficientes y apropiados para que la organización pueda ejercer su responsabilidad en lo que respecta a la supervisión del riesgo tecnológico, independientemente de sobre qué recurso tecnológico se materialice; (ii) el uso de una estrategia de supervisión que resulte eficiente tanto a la hora de supervisar recursos tecnológicos desplegados usando un modelo de computación en la nube como para supervisar otras tipologías de ecosistemas tecnológicos, y (iii) la integración de los procesos de aseguramiento sobre todos estos recursos para ofrecer una visión unificada que permita una priorización y tratamiento consistente de los riesgos tecnológicos en la organización.

El primer pilar, consistente en la dotación de recursos, parte de la función de auditoría interna de TI, como responsable de la supervisión de los riesgos tecnológicos de la organización, y se desarrolla a través de la asignación y definición de roles que asocien los principales perfiles a cargo de la función de auditoría interna de TI con las principales actividades que resultará necesario ejecutar para ofrecer aseguramiento tanto sobre los servicios cloud contratados, como sobre el resto de la tecnología. Junto con dichas responsabilidades, también se identifican todas las herramientas y elementos clave de supervisión necesarios para ofrecer aseguramiento.

El segundo pilar, que se centra en la estrategia de supervisión, se ha desarrollado a partir de los procesos tradicionales de auditoría y monitorización continua (CA&CM). A su vez, CA&CM se descompone en procesos de aseguramiento continuo de controles (CDA), monitorización continua de controles (CCM), y monitorización y evaluación continua de riesgos (CRMA). Cada uno de ellos descrito con un enfoque doble de supervisión de recursos internos y de supervisión de recursos cloud, siendo extensible el enfoque cloud a cualquier recurso externalizado en la medida en la que se adapten los elementos clave de supervisión a las características de dicho recurso.

El tercer y último pilar, que asegura la consolidación de reportes, permite ofrecer aseguramiento sobre los riesgos tecnológicos de la organización con un enfoque centrado en el riesgo y ofreciendo abstracción sobre los recursos, para garantizar que los riesgos son evaluados y tratados de forma consistente. Para ello, se ha diseñado un modelo de supervisión que ofrece abstracción de los riesgos sobre los recursos sin que se produzca pérdida de trazabilidad entre ellos, para favorecer un tratamiento eficiente de éstos.

A lo largo de los siguientes capítulos, se desarrollará el modelo de auditoría y monitorización continua para organizaciones que hagan uso de servicios cloud, sin limitar la supervisión a los servicios cloud exclusivamente, para que puedan cubrirse todos los riesgos tecnológicos a los que los recursos TI de la organización se ven expuestos.

De esta forma, el Capítulo 2 se dedica a una descripción generalista de CA&CM. En él, se lleva a cabo una exposición general de los procesos de CA&CM sobre los que posteriormente se desarrollará el modelo de supervisión, y se exponen los retos y beneficios esperados de este modelo. A continuación, en el Capítulo 3, se describen con mayor nivel de detalle los procesos que forman parte del modelo de CA&CM, y se identifican aquellos aspectos que es necesario considerar para lograr su integración tanto en recursos desplegados dentro de la organización, como para integrarlos con servicios cloud. Por tanto, para cada proceso que forma parte de CA&CM, se incorpora una justificación de su utilidad en cloud, los retos a los que se enfrenta la organización para lograr la integración, los elementos clave del proceso en recursos on premise y cloud, y claves y mejores prácticas para su integración.

En el Capítulo 4, asociados a cada uno de los procesos que componen CA&CM, se describen los elementos clave de supervisión que deben desplegarse para darles soporte. Éstos variarán dependiendo de los objetivos de cada proceso. De esta forma, CDA, cuyo elemento clave de supervisión es la analítica de datos, se fundamenta en los procesos y reglas de negocio, que a su vez dan lugar a procesos de gestión de Información. CCM, por su parte, se basa en la evaluación continua de controles y KPIs, que dependen de los objetivos de ciberseguridad y de negocio

que se hayan definido. Por último, CRMA se fundamenta en el análisis de KRIs, integrados en un proceso de análisis de riesgos a partir del mapa de riesgos obtenido del análisis de los contextos interno y externo de la organización.

Todos los procesos y elementos clave de supervisión descritos en los capítulos 3 y 4, se integran a lo largo del Capítulo 5. En este capítulo se definen las estrategias de ejecución y evolución de los procesos de CA&CM. Por un lado, la estrategia de ejecución está basada en un modelo iterativo soportado por principios ágiles de gestión. Por otro lado, la evolución del modelo se logra mediante la introducción de modificadores sobre las fases del modelo de iteración, a medida que las necesidades de supervisión van cambiando como resultado de la ejecución sucesiva de iteraciones y el incremento en la madurez de la supervisión.

Finalmente, en el Capítulo 6 se identifican las principales conclusiones obtenidas fruto del desarrollo del modelo de supervisión de organizaciones que hacen uso de servicios cloud basado en procesos de CA&CM. Entre las conclusiones, destacan las reflexiones respecto de la mejor integración de los recursos cloud en la supervisión fruto de los procesos de CA&CM, así como el incremento en la eficiencia de la función de auditoría TI producto de la integración de CA&CM con la ejecución de auditorías tradicionales.

2 Auditoría Continua y Monitorización Continua (CA&CM)

2.1. Descripción de CA&CM.

Los dos conceptos clave que definen la auditoría y monitorización continua (CA&CM) son la evaluación soportada por técnicas de automatización, y el incremento en la frecuencia de análisis. Adicionalmente, existe un cambio en el enfoque de evaluación en el que se prescinde del uso de técnicas de muestreo para sustituirlas por una evaluación completa de la población auditada.

En CA&CM, además, se modifica el enfoque de reporte para que éste se apoye en técnicas que faciliten la integración con la toma de decisiones y supervisión de los órganos de gobierno y control, gracias al uso de técnicas de representación de datos como la representación histórica de tendencias gracias al uso de Indicadores Clave de Desempeño (KPIs) o Indicadores Clave de Riesgo (KRIs), o al uso de Balanced Scorecard (BSC).

El uso de este enfoque, basado en un análisis continuo sobre la población completa de elementos, que además hace uso del análisis evolutivo y de tendencias, ayuda a la función de auditoría interna a adquirir un entendimiento más completo de los riesgos en la organización y de los puntos de control críticos, así como a identificar más fácilmente las reglas y excepciones presentes en los procesos auditados.

El objetivo último de CA&CM es poder evaluar tanto los controles y los riesgos en tiempo real, o al menos de forma suficientemente continua como para tener visibilidad constante del riesgo al que se ve expuesta la organización, pudiendo asegurar un tratamiento más eficiente y con una exposición al riesgo menor. Si bien CA&CM no está necesariamente ligado a la función de audi-

toría TI y puede integrarse con otras funciones a cargo de la supervisión de riesgos y controles, a efectos del presente trabajo se utilizará de forma exclusiva para la evaluación de riesgos de carácter tecnológico. Esto supone que de las dos funciones básicas de CA&CM, consistentes en ofrecer aseguramiento mediante la ejecución de auditorías, y el aseguramiento directo a los miembros de la Dirección, se desarrollarán los procesos para dar soporte a la auditoría continua (CA).

Implantar CA&CM requiere la ejecución de 3 procesos de supervisión: Aseguramiento Continuo de Datos (CDA), Monitorización Continua de Controles (CCM), y monitorización y evaluación continua de riesgos (CRMA). El objetivo del Aseguramiento Continuo de Datos es monitorizar la calidad de la información utilizada por los procesos clave de la organización, para asegurar que la organización haga uso de información correcta. La Monitorización Continua de Controles permite validar la efectividad de los controles desplegados en la organización. Por último, la Monitorización y Evaluación Continua de Riesgos permite asegurar que los riesgos se encuentren en todo momento dentro de los niveles aceptables esperados.

2.2. Retos generales en la aplicación de CA&CM en la organización.

2.2.1. Será necesario obtener y mantener el apoyo del Comité de Auditoría y de la Dirección para la ejecución de CA&CM, que resulta más costoso que la ejecución de auditorías tradicionales, y requiere un proceso de adaptación de los equipos de auditoría en el que el aporte de valor de estas actividades será reducido.

2.2.2. Respecto de la aplicación de CA&CM en cloud, aunque muchos contratos proveedores ya incorporan cláusulas de auditoría (right-to-audit), el volumen de información que deberá facilitar el CSP para implementar CA&CM es mayor que para la ejecución de otro tipo de auditorías, y la coordinación que debe establecerse con el CSP mayor, lo que puede entrañar dificultades durante la negociación del contrato.

2.2.3. La mayor dificultad a la hora de implantar CA&CM está asociada a la necesidad de automatizar la ejecución de evaluaciones de riesgos y controles, que requiere de un elevado conocimiento técnico y tiempo para el desarrollo de las pruebas automatizadas.

2.2.4. De manera particular, para la ejecución de analítica de datos, como parte del proceso de aseguramiento continuo de datos, la función de auditoría interna deberá contar con perfiles especializados, y deberá soportar su actividad en herramientas específicas de analítica de datos, debiendo incurrir en costes adicionales.

2.2.5. CA&CM requiere una mayor involucración de las áreas, dado que la interacción con éstas es más frecuente, y la información y feedback que éstas deberán proporcionar es mayor, lo que podría generar fricción con dichas áreas.

2.2.6. Para que los procesos de CA&CM aporten valor a la organización sus resultados deben integrarse en los procesos de decisión del resto de la organización, lo que implica que debe existir un elevado compromiso con la adopción de CA&CM por parte de los perfiles a cargo de las principales áreas de la organización.

2.2.7. Con CA&CM, ciertos procesos dentro del flujo de supervisión se vuelven más complejos, y dicha complejidad debe ser gestionada, debiendo prestar especial atención a este respecto a los procesos de reporte y seguimiento de conclusiones y recomendaciones.

2.2.8. Para que un incremento en el volumen de información utilizada para la supervisión no conlleve la emisión de conclusiones incorrectas, debe prestarse especial cuidado a obtener dicha información exclusivamente de fuentes fiables.

2.2.9. Dado que la automatización nunca podrá ser completa a la hora de ejecutar CA&CM en un modelo en el que se persigue su integración con otros procesos de aseguramiento, podría producirse una situación en la que la falta de automatización de determinadas actividades provocara un consumo de recursos que impidiera el aporte de valor de este modelo de supervisión.
2.2.10. Si los reportes generados no están suficientemente procesados y adaptados a la audiencia objetivo, el aporte de valor de CA&CM se verá reducido.

2.3. Consideraciones mínimas para poder aplicar CA&CM.

2.3.1. El equipo de auditoría debe poseer el conocimiento suficiente como para ejecutar y automatizar hasta un nivel aceptable los procesos que componen CA&CM.

2.3.2. La información utilizada por los procesos de CA&CM debe cumplir con unos requerimientos mínimos de calidad, y ser obtenida de fuentes fiables.

2.3.3. El nivel de automatización de los procesos de CA&CM debe ser el suficiente como para que su ejecución sea costo-efectiva.

2.3.4. Deben ejecutarse procesos de normalización de información para que, aunque ésta se obtenga de fuentes heterogéneas, pueda ser integrada en los procesos de CA&CM de forma eficiente.

2.3.5. Los procesos de recopilación automatizada de información deben diseñarse de forma que no comprometan el funcionamiento normal de los sistemas desde los que se obtenga dicha información.

2.3.6. Debe adquirirse una elevada comprensión de los procesos de negocio como para que el análisis de información, controles y riesgos tenga en cuenta los requerimientos y características de dichos procesos, y los resultados obtenidos se contextualicen adecuadamente.

2.3.7. Es necesario identificar las fuentes más eficientes desde las que obtener la información y aquellos puntos clave de los procesos en los que evaluar cada uno de los riesgos y controles analizados.

2.3.8. El conjunto de elementos clave a supervisar seleccionado debe ser coherente y consistente, de forma que permita emitir conclusiones robustas sobre los riesgos y controles evaluados.

2.3.9. Las excepciones y desviaciones identificadas durante el análisis deben ser investigadas y entendidas, de forma previa a su reporte, para garantizar que se reportan hechos relevantes para la organización.

2.3.10. Debe ofrecerse una visión acumulada y cuantificada sobre la exposición total de la organización al riesgo, de forma que se evite ofrecer conclusiones parciales o sesgadas.

2.3.11. Los procesos de CA&CM deben ser analizados periódicamente, de forma que se modifiquen cuando se detecten aspectos que deben ser corregidos.

2.3.12. A la hora de seleccionar los elementos clave de evaluación para un determinado control o riesgo, así como para determinar la periodicidad con la que se lleven a cabo las evaluaciones, debe considerarse un enfoque que sea costo-efectivo y que tengan en cuenta la exposición de la organización al riesgo asociado.

2.3.13. Fruto de los procesos de CA&CM, o de la ejecución posterior de auditorías que utilice la información producida por éstos como input, debe priorizarse la ejecución de acciones que aseguren el tratamiento de los riesgos identificados, puesto que el aseguramiento no puede acabar en la identificación de los riesgos.

2.3.14. Es fundamental mantener la integridad de los procesos de CA&CM, de manera que no se lleven cambios no controlados sobre éstos que puedan comprometer la validez de las conclusiones obtenidas.

2.4. Beneficios esperados al aplicar CA&CM en Cloud.

2.4.1. Reducción en la probabilidad de ocurrencia de fraude y errores en la ejecución de procesos y procesamiento de información.

2.4.2. Uso más eficiente de la información disponible en la organización, al integrar un mayor volumen de ésta en los procesos de aseguramiento.

2.4.3. Obtención de mayores niveles de cumplimiento regulatorio, siempre que los requerimientos correspondientes sean tenidos en cuenta y se integren en el proceso de supervisión.

2.4.4. Se incrementa el aseguramiento ofrecido al Comité de Auditoría y a la Dirección, al ofrecer una visión continua de los riesgos y del entorno de control de la organización, en lugar de un enfoque puntual y de alcance más limitado.

2.4.5. Ofrece un mayor soporte a la hora de definir el plan anual de auditoría, puesto que permitirá centrar las auditorías sobre aquellos riesgos y controles que presenten anomalías o que resulten más críticos para la organización, a partir de los resultados de la ejecución de CA&CM.

2.4.6. Reduce el tiempo de respuesta desde que una parte interesada de la organización expone una inquietud a la función de auditoría interna hasta que dicha función expone conclusiones con respecto a dicha inquietud, aunque posteriormente dichas conclusiones puedan ser complementadas con trabajos de mayor profundidad.

2.4.7. Incorpora una capa de control adicional en la organización, que sirve de abstracción, entre las capas técnicas y operativas de la organización, y la función de auditoría. Aunque dicha abstracción nunca llega a ser completa, y las auditorías que se ejecuten deben ser suficientemente detalladas como para poder emitir una opinión válida, CA&CM favorece una ejecución más eficiente y dinámica de éstas.

PROCESOS CLAVE 3

3.1. Aseguramiento continuo de datos (CDA).

Tradicionalmente, el aseguramiento continuo de datos (CDA, por sus siglas en inglés), se asocia al análisis de datos y transacciones de carácter financiero, destinado a garantizar que éstos se mantienen íntegros. Esto se debe tanto a la importancia de este tipo de información, como a la limitación que tradicionalmente ha existido a la hora de analizar grandes volúmenes de información, lo que ha restringido la capacidad de las organizaciones de extender este tipo de análisis a otras tipologías de información.

Sin embargo, con la introducción de técnicas como el análisis basado en Big Data o el tratamiento distribuido de información, así como por las capacidades de procesamiento bajo demanda introducido por los servicios en la nube, se incrementan las posibilidades de realizar análisis continuo de datos sobre otras tipologías de información.

3.1.1. Por qué CDA en Cloud.

- Con el incremento en los ecosistemas tecnológicos producido en parte por la adopción de servicios cloud se generan volúmenes de información que es necesario tratar.
- Se incrementa la volatilidad de los datos, lo que requiere un análisis constante, o al menos con una frecuencia alta, de los elementos críticos.
- Permite la detección de patrones anómalos de comportamiento de los usuarios, lo que en un entorno más complejo como en las arquitecturas cloud resulta necesario para mantener la visibilidad sobre los riesgos.
- Ayuda a asegurar el cumplimiento de aquella regulación que tiene un impacto directo en los datos gestionados por la organización.

3.1.2. Retos.

- La instalación de herramientas para el análisis de la integridad de la información en reposo en los entornos cloud puede resultar complejo.
- Existe cierta dificultad para analizar todo el tráfico de red hacia/desde el entorno a causa de: (i) acceso distribuido desde host no controlados, (ii) volúmenes de información generados, y (iii) visibilidad sobre la red.
- No es posible llevar a cabo analítica de datos sobre información cifrada, por lo que la protección del a información podrá dificultar su análisis.
- Se incrementa la dificultad a la hora de asegurar máxima visibilidad sobre los datos. En el entorno cloud se posee un acceso más directo a los datos. Sin embargo, existen mayores restricciones a la hora de instalar y ejecutar herramientas de análisis de datos. En cambio, en la infraestructura propia, la instalación de herramientas es más fácil, pero se pierde cierta visibilidad sobre los datos almacenados en la nube.
- Deben crearse reglas para la detección de anomalías basadas en información transmitida en red que permitan detectar riesgos, lo cual requiere una inversión considerable de tiempo y recursos.
- Debe encontrarse un punto de equilibrio en el que no se analice el 100% de la información, y CDA siga aportando valor a la organización.
- Al tratarse de un servicio cloud, existe cierta elasticidad que permitirá a las actividades de CDA ejecutarse sin problema sin que afecte al funcionamiento "operativo" del entorno. Sin embargo, esto también puede introducir costes imprevistos en caso de que se produzca una carga de procesamiento excesiva fruto del análisis.
- La ejecución de procesos adicionales sobre el entorno cloud puede provocar la introducción imprevista de vulnerabilidades sobre éste.

3.1.3. Elementos clave.

- El análisis de la información, así como la opinión sobre ésta debe ser constante, o al menos periódica en el tiempo, y no realizarse de forma puntual.

- El análisis de la información, así como la opinión sobre ésta debe ser constante, o al menos periódica en el tiempo, y no realizarse de forma puntual.

- La información obtenida por CDA debe permitir analizar las tendencias y evolución a lo largo del tiempo, por lo que no debe basarse en un modelo binario de evaluación (Ok/KO).

- Los procedimientos básicos incluidos dentro de CDA comprenden la verificación de la información maestra, así como las transacciones ejecutadas.

- Otros aspectos que también es apropiado analizar es la transferencia al entorno de datos cuya clasificación no permita su almacenamiento fuera de sistemas corporativos, o que por la localización del datacenter del distribuidor, no puedan alojarse en éste. En este caso, no se busca tanto garantizar la integridad de los datos, sino su confidencialidad.

- Puede recurrirse al análisis continuo de datos para realizar una validación indirecta del funcionamiento de los controles implementados sobre éstos, garantizando que dichos datos se mantienen correctos, con niveles de calidad apropiados, y que cumplen en todo momento con las reglas de negocio asociados a éstos.

- La opinión debe representarse de forma que se abstraiga la complejidad asociada al análisis y se muestren de forma clara y sintética en lo que respecta al impacto para el negocio de la conclusión alcanzada.

- Aunque el proceso de CDA puede automatizarse utilizando herramientas de analítica de datos y ejecución programa de scripts, es conveniente que las áreas de negocio realicen validaciones periódicas sobre los reportes obtenidos, tanto para detectar nuevas casuísticas no contempladas, como para adaptarlos a los cambios en los requerimientos de negocio.

  Adaptar la capacidad de aseguramiento de datos al entorno y los recursos, incluyendo:
  a. Saber qué datos y actividades son críticas.
  b. Saber qué modificaciones de los datos son especialmente relevantes.
  c. Establecer niveles de tolerancia al cambio, dependiendo de la criticidad y función de cada dato.

- Debe priorizarse la seguridad del a información frente a la capacidad de ejecución de CDA. No es conveniente prescindir del cifrado, microsegmentación, etc., solo para poder ejecutar CDA.

- Como criterio para la identificación de datos críticos, debe prestarse especial atención a la clasificación de los datos según el esquema de clasificación de la información definido, así como a los requerimientos regulatorios impuestos sobre ellos.

3.1.4. Cómo implementar CDA.

- CDA sobre un servicio cloud debería ejecutarse preferiblemente en cloud, de forma que solo el resultado del análisis se vuelque a local.

- Dedicar el tiempo suficiente a entender los datos clave a analizar, su comportamiento esperado, y crear estratégicas adaptadas a cada uno de ellos. No es conveniente analizar todas las tipologías de datos de la misma manera o sin considerar criterios propios de la organización, simplemente comprobando parámetros estándar de calidad.

- Diseñar patrones de comportamiento totalmente adaptado a los datos almacenados y a la actividad de los usuarios con éstos.

- CDA en cloud debe ser especialmente adaptable para no incurrir en costes extra no controlados, de forma que el análisis se ajuste dinámicamente a las capacidades del entorno.

- Deben identificarse los puntos dentro de los procesos donde es necesario ejecutar CDA para asegurar la validez y eficiencia de la supervisión sin sobrecargar excesivamente la capacidad del entorno.

- CDA debe integrarse también con los sistemas on premise de la organización y la información almacenada en éstos. Esto permitirá un análisis mucho más profundo de la información y un aporte de valor mayor, puesto que, tanto para el análisis de calidad de datos, como para la detección de anomalías, analizar un mayor número de sistemas integrados permite obtener resultados más precisos.

- Aunque tradicionalmente CDA se ha ocupado de analizar información financiera y comportamientos anómalos en relación con ésta, deben identificarse otros fines para los que este proceso resulte útil dentro de la gestión de riesgos de TI, como por ejemplo para la detección temprana de APTs.

- La selección de los datos analizar con CDA debe partir de un análisis del riesgo integral y multi-dimensional, que tenga en cuenta no solo riesgos financieros, sino también de cumplimiento, tecnológicos, operativos, etc. Esto favorecerá que el proceso satisfaga las expectativas de la organización.

- Utilizar un enfoque top-down a la hora de definir las actividades de CDA, lo que ayudará a crear una estrategia más coherente y a asegurar las expectativas de las partes interesadas.

- Utilizar un enfoque iterativo y que permita ir incrementando la supervisión a medida que se va obteniendo experiencia e información que retroalimente el proceso.

3.2. Monitorización Continua de Controles (CCM).

La función básica del proceso de monitorización continua de controles es la de asegurar el cumplimiento con las políticas y procedimientos de la organización, y garantizar que los procesos operan adecuadamente. Otra de sus características habituales es que este objetivo debe alcanzarse mediante el análisis automatizado de controles. Para ello, deben elegirse un conjunto de controles críticos, que serán evaluados teniendo en cuenta las reglas de negocio que apliquen sobre los procesos sobre los que éstos se implementan. Gracias a este tipo de análisis, es posible detectar de forma temprana la ocurrencia de anomalías o excepciones para su análisis posterior. Uno de los elementos básicos utilizados en este proceso son los KPIs, que permiten analizar la evolución de indicadores clave a lo largo del tiempo y ayudan a detectar anomalías como resultado de su medición y comparativa histórica.

3.2.1. Por qué CCM en Cloud.

- El uso de servicios cloud, así como el incremento en el número y heterogeneidad de los sistemas de información utilizados por una organización, provocan una reducción en la periodicidad con la que estos sistemas pueden ser revisados de forma manual por parte de los equipos de auditoría de TI. Por ello, es necesario establecer una fase de triaje de sistemas previa que permita identificar aquellos que están expuestos a un mayor riesgo como resultado del funcionamiento de los controles implementados sobre éstos.

- Al igual que ocurre con CDA, el incremento en el volumen de información disponible, tanto interna como externa, requiere una aproximación continua, que reduzca el volumen de información a tratar en cada análisis, de forma que se distribuya el esfuerzo lo más homogéneamente posible a lo largo del tiempo.

- Con el incremento en la regulación en materia de protección de datos, privacidad y ciberseguridad, se produce un aumento en el número de revisiones que es necesario realizar de forma obligatoria. Haber implementado un proceso de CCM ayuda a acreditar frente a un tercero la debida diligencia en el cumplimiento de los requerimientos de supervisión impuestos por las diversas regulaciones.

- En la medida en la que determinados controles se implementen de forma similar sobre diversos sistemas, o al menos dejen trazas similares de su ejecución, la implementación de CCM supondrá una reducción en el coste de supervisión, a raíz de la automatización y estandarización de las revisiones.

3.2.2. Retos.

- Resulta complicado recopilar toda la información relevante para el análisis procedente del entorno cloud. La dificultad se incrementará en la medida en la que el tipo de análisis se vuelva más técnico, siendo más fácil obtener la información necesaria para aplicar CCM sobre un proceso que sobre la infraestructura tecnológica, porque esto requerirá obtener información que normalmente no está a disposición del cliente del servicio.

- Como ya ocurría con CDA, adquirir toda la información requerida por el proceso de CCM de forma que el cliente del servicio pueda analizarla puede resultar costoso, e incluso inseguro si esta se transmite a través de una red pública sin la adecuada protección.

- Pueden surgir discrepancias en los requerimientos asociados al funcionamiento de los controles, y en última instancia el riesgo aceptable, entre entornos desplegados on premise y los servicios en la nube. Existen diversas limitaciones presentes a la hora de gestionar y supervisar estos servicios que pueden impactar tanto en el diseño del proceso de CCM como en su operación posterior.

- Existe una cuestión básica asociada con la capacidad de control que es necesario tener en cuenta a la hora de seleccionar los controles que se incluirán dentro del proceso. Dependiendo del modelo del servicio y del proveedor (CSP), la responsabilidad de la im-

plantación y la gestión de controles recaerá en algunos casos en el CSP y en otros casos en el cliente. Por tanto, surge la cuestión de si deben incluirse en el proceso aquellos controles sobre los que el cliente del servicio no tiene capacidad de gestión, y por tanto configuración, u operación. A pesar de que su inclusión ofrece una perspectiva más amplia del estado del riesgo asociado al servicio, también puede ofrecer una visión poco realista sobre la gestión que el cliente hace del riesgo, al incluir controles sobre los que no tiene capacidad de actuación.

- En última instancia, hacer uso de CCM requiere una monitorización continua de controles. El nivel de complejidad a la hora de implementar este proceso sobre controles de TI puede ser muy elevado, a causa de su heterogeneidad y de la complejidad de su análisis. Automatizar la adquisición de las evidencias de auditoría correspondientes como su posterior análisis puede requerir de un alto esfuerzo, dependiendo del control a analizar.

- Este tipo de análisis puede generar unas expectativas en las áreas de Negocio y Órganos de Gobierno difíciles de cumplir, especialmente al involucrar servicios en la nube, sobre la capacidad de supervisión y actuación asociada a dicho servicio.

- El nivel de conocimiento y especialización requerido para la automatización del análisis de controles es muy elevado, a causa de la heterogeneidad de servicios y la diversidad de configuraciones y modelos de despliegue.

3.2.3. Elementos clave.

- Durante la selección de los controles a integrar en CCM deben considerarse las posibilidades de automatización de cada uno de ellos, a partir de sus características técnicas y de los recursos a disposición de la organización.

- Como mínimo, los controles a analizar deben abarcar los siguientes aspectos:

  a. Cumplimiento regulatorio por parte del cliente en relación con los aspectos gestionados en el servicio cloud o relativos a la propia infraestructura.
  b. Gestión del CSP de la infraestructura tecnológica.
  c. Gestión del servicio cloud por parte del CSP.
  d. Operación de la infraestructura / servicio cloud
  e. Control / Protección del servicio cloud por parte del cliente en el propio entorno
  f. Control / Protección del servicio cloud desde la infraestructura del cliente
  g. Gobierno del servicio Cloud.

- Incluir cláusulas en el contrato con el CSP que aseguren la correcta ejecución de estas actividades, tanto en lo que respecta a la preparación del entorno y recopilación de información por parte del cliente, como en la colaboración que resultará necesaria por parte del CSP.

- Al incrementar el número de revisiones, también se incrementa el número de reportes. En última instancia, para muchos de los controles analizados esta revisión es continua, por lo que es imprescindible ofrecer un modelo de representación de resultados que permita extraer conclusiones de forma rápida y sencilla, sin que deba hacerse uso de un procesamiento posterior, salvo que se desee indagar en un aspecto concreto a raíz de los resultados obtenidos.

- Un proceso de CCM nunca podrá sustituir al resto de análisis llevados a cabo por la función de auditoría interna. Por ello, aunque CCM puede servir como input a dicha función, es importante que a partir de ésta se lleven a cabo auditorías para identificar y tratar los riesgos asociados al servicio en la nube.

- Como ocurre con otras actividades asociadas a la función de aseguramiento, es importante basarse en estándares y buenas prácticas reconocidas. Por ello, un elemento clave a la hora de definir el proceso de CCM es utilizar un marco de control que se adapte al servicio cloud. Existen diversas alternativas, entre las que destacan Cloud Control Matrix, de CSA; o la Norma ISO/IEC 27017.

3.2.4. Cómo implementar CCM.

- Aunque el objetivo último de CCM sea lograr un análisis continuo, este objetivo no es razonable desde el primer momento, y es conveniente tener en cuenta que un análisis periódico es preferible a uno puntual, por lo que es mejor centrarse en lograr incrementar la periodicidad de los análisis de forma progresiva, que en lograr una automatización completa desde el inicio.

- Existirán algunos controles que por su tipología o características técnicas no sean automatizables. En estos casos, deberá evaluarse su relevancia a la hora de determinar el riesgo para la organización. En caso de que no aporten información relevante, o haya algún control alternativo que ofrezca la misma información, podrán descartarse. Por el contrario, si aportan información relevante, deberá incluirse como un control de revisión semiautomática o manual.

- Aunque inicialmente no debería existir una limitación a la hora de incluir controles en las categorías de revisión automática, semiautomática, o manual. No obstante, a medida que se vayan producido iteraciones del proceso, deberá tratarse de llevar el mayor número de controles a un análisis automático, dejando el menor número posible en revisión manual.

- A medida que un mayor número de controles pasen a monitorizarse de forma automática, se podrá incrementar el número de controles de supervisión semiautomática o manual dentro del proceso, pudiendo aumentar el alcance de la revisión a ámbitos de controles cuya automatización no sea viable.

- Además de intentar incrementar el grado de automatización, es conveniente realizar un análisis periódico que permita identificar lo siguiente:

    a. Los controles incluidos dentro del proceso son los adecuados a partir de sus características (posibilidad de análisis automatizado, recurso sobre el que se implementan, consistencia con respecto del resto de controles, etc.).
    b. Los controles incluidos dentro del proceso aportan información relevante sobre los riesgos.
    c. Existencia de controles adicionales que deban incluirse por existir riesgos relevantes que no estén cubiertos actualmente.
    d. Controles alternativos o complementarios a los actuales cuya inclusión suponga un incremento relevante en la capacidad de supervisión del entorno cloud o que faciliten el proceso de automatización de su revisión.
    e. Los controles se están revisando de forma adecuada, y las variaciones significativas en las mediciones periódicas implican anomalías relevantes que afectan al riesgo y que es necesario considerar.

- Puesto que los entornos cloud, especialmente aquellos que ofrecen un servicio de tipo IaaS, permiten la implantación de herramientas de control propias, y muchas de ellas poseen funcionalidades de envío remoto de reportes, es conveniente, para no sobrecargar el entorno gestionar, la recopilación y envío de información que nutra el proceso de CCM desde el entorno cloud, y realizar el análisis posterior en un entorno propio, para no sobrecargar la capacidad de cómputo del entorno Cloud.

- Es conveniente que este proceso se diseñe desde las fases de adopción y selección de servicios en la nube, de forma que, para aquella información que deba proporcionar el CSP, exista un acuerdo sobre la periodicidad y características de la información que el proveedor reportará al cliente como entrada al proceso de CCM.

- Es importante llevar a cabo una labor de concienciación a nivel interno que permitan a los Órganos de Gobierno y al resto del Negocio entender los requerimientos y resultados del proceso de CCM. En general, es más probable que el retorno sobre la inversión se produzca como resultado de un mejor análisis y aproximación al tratamiento del riesgo que por la necesidad de menores recursos para la ejecución de CA&CM.

3.3. Monitorización y evaluación continua de riesgos (CRMA).

Utilizando como información de partida aquella resultante de los dos procesos vistos anteriormente, así como mediante la definición y análisis de KRIs construidos a partir del mapa de riesgo corporativo, la monitorización y evaluación continua de riesgo permite integrar estos procesos con el proceso de análisis de riesgos de la organización e incluso con el diseño del plan anual de auditoría, facilitando la asignación de recursos a aquellas áreas, procesos o activos con mayor riesgo, y priorizando la ejecución de auditorías sobre aquellos procesos o sistemas que posean riesgos más elevados. Posteriormente, esta información también será útil durante las fases de evaluación preliminar dentro del trabajo de auditoría, para identificar la situación del proceso y los controles a auditar; y durante el diseño del programa de trabajo, que debería cubrir entre otros aspectos aquellos indicadores con peores resultados.

3.3.1. Por qué CRMA en Cloud.

- El uso de un servicio sustentado en una infraestructura que no está bajo el control directo de la organización, y que en muchos casos se contrata sin ofrecer la adecuada visibilidad dentro de la organización (Shadow IT) dificultan la gestión de los riesgos asociados a éste. El uso de CRMA favorece una mayor transparencia y visibilidad sobre la gestión del riesgo en el entorno cloud, contrarrestando así la pérdida de visibilidad inherente a su uso.

- Existen riesgos introducidos en la organización de forma directa por el uso de recursos externos, así como otros específicos a los servicios cloud, por las particularidades en su arquitectura tecnológica. Dado que en ambos casos se produce una reducción en la capacidad de control, el uso de CRMA ayudará a paliar este hecho con una supervisión más estrecha y directa de los riesgos.

- La implementación de CRMA sobre un servicio que está sujeto a cambios imprevistos por parte del proveedor facilita la adaptación de la organización a dichos cambios.

- CRMA ofrece una visión actualizada y precisa, al basarse en la medición y análisis de KRIs, del riesgo para la organización del uso de servicios cloud, y permite integrar esta visión con la del resto de riesgos de la organización usuaria del servicio de forma más sencilla.

3.3.2. Retos.

- Si bien la definición de KRIs no debería ser compleja para un servicio en la nube, su medición puede entrañar ciertas dificultades, especialmente en lo relativo a aquellos riesgos asociados a la gestión y control del CSP sobre el servicio o la infraestructura que le da soporte.

- El tratamiento de aquellos riesgos que se consideren por encima del umbral aceptable puede requerir la interacción con el CSP, lo que puede resultar un problema si a nivel contractual no se han definido las obligaciones de ambas partes asociadas a dicho tratamiento.

- Integrar la gestión del riesgo del servicio con el resto de los riesgos corporativos requiere dar visibilidad del servicio a las áreas de control involucradas. Aunque la gestión de recursos tecnológicos debería estar centralizada, los servicios cloud facilitan la aparición de recursos "no declarados" (Shadow IT), por lo que las áreas de control no siempre son conocedoras de todos los recursos TI de los que dispone la organización, ni del uso que las áreas hacen de éstos.

- La definición de KRIs, especialmente sobre el servicio en la nube, puede ser completa a causa tanto de las particularidades de este entorno como de la falta de conocimientos técnicos de una tecnología cuya aparición puede ser considerada reciente si se compara con el resto de las arquitecturas tecnológicas utilizadas por las organizaciones.

3.3.3. Elementos clave.

- Aunque este proceso se encarga de la monitorización del riesgo, es necesario haber definido un mapa de riesgos suficientemente completo, que incluya riesgos de los siguientes ámbitos:

    a. Riesgos internos a la organización que contrata los servicios en la nube.
    b. Riesgos internos asociados al CSP.

c. Riesgos externos asociados a los entornos en los que opera la organización y el CSP.
d. Riesgos de baja probabilidad y alto impacto (cisnes negros) que puedan afectar al servicio en la nube o a la organización.

- Como mínimo, CRMA debería considerar riesgos asociados al servicio cloud y de forma global a la organización que cubrieran las siguientes tipologías:

  e. Cumplimiento regulatorio
  f. Estratégicos
  g. Operativos
  h. Técnicos (incluyendo riesgos de ciberseguridad).
  i. Financieros

- Este proceso debe hacer uso de indicadores clave de riesgo (KRIs) y métricas de riesgo que se evalúen de forma periódico.

- Si bien CCM y CDA en general requiere la automatización de actividades, el proceso de CRMA requiere además la definición de algoritmos o heurísticas que permitan extraer conclusiones sobre el nivel de los riesgos a partir de las mediciones realizadas y resultados de los otros dos procesos.

- Es necesario lograr la comunicación y cooperación entre las funciones de gestión de riesgo de la organización y la función de aseguramiento para la definición y gestión del proceso de CRMA.

- Utilizar un sistema de reporte que ofrezca vistas dinámicas dependiendo del grupo de reporte, de forma que se ofrezca mayor detalle al responsable de la gestión del riesgo o a la función de auditoría interna, y se aporte una visión más agregada o de alto nivel si los destinatarios de un determinado reporte son los miembros del algún órgano de gobierno.

3.3.4. Cómo implementar CRMA.

- Puesto que el contacto con el CSP debe realizarse de forma coordinada, así como las actividades que ofrezcan aseguramiento, para evitar la fatiga de auditoría, producida por la repetición de actividades similares o que se solapan, es importante que este proceso integre a todas las unidades de la organización que requieran visibilidad sobre los riesgos a los que la organización está expuesta como resultado de la adopción del servicio cloud.

- Los KRIs que se definan para evaluar el servicio cloud y el riesgo que éste supone para la organización deben orientarse para facilitar la identificación de la causa raíz de los riesgos evaluados.

- Identificar el número adecuado de KRIs a analizar, de forma que sean los suficientes como para identificar los principales riesgos, pero no tantos como para que su análisis no sea costo-efectivo, teniendo especial cuidado en lo seleccionar KRIs con un solapamiento elevado entre sí, y priorizando aquellos que ofrezcan una cobertura mayor y aporten información de mayor relevancia para el análisis.

- El proceso de CRMA en cloud, como en cualquier otro entorno tecnológico u organizativo, debe estar integrado con los procesos de CCM y CDA, puesto que, por sus características, se requiere una provisión continua de información de entrada como resultado de la ejecución de los otros dos procesos. De no ser así, no se dispondrá de la información suficiente como para llevarlo a cabo de forma eficiente.

- Tan importante con incluir dentro del proceso los riesgos asociados al uso de la nube es adoptar un enfoque global a la organización, de forma que los riesgos del servicio queden adecuadamente contextualizados y se realice una correcta asignación de recursos a partir de la priorización completa de todos los riesgos de la organización.

- CRMA debe integrarse con la función de aseguramiento llevada a cabo por el área de Auditoría Interna, de manera que la ejecución de auditorías, que nunca podrá ser sustituida de forma completa por CRMA, se nutra de la mayor cantidad posible de información.

- De todos los procesos analizados en este apartado, CRMA es el que interactúa de forma más directa con los órganos de gobierno y control de la organización, por lo que es importante mantener una comunicación periódica y adaptada con éstos en la que se prioricen los resultados de la ejecución de CRMA frente a la de los otros dos procesos de CA&CM.

- Para que las partes interesadas puedan extraer el máximo de información, y teniendo en cuenta que el resultado de esta actividad puede llegar a los máximos responsables de la organización, es importante que se generen reportes fácilmente comprensibles y que muestren información relevante sobre la situación de los riesgos analizados.

- La inclusión de riesgos asociados al CSP (gestión del CSP del servicio, de las obligaciones regulatorias o de la infraestructura utilizada para proveer el servicio -almacenamiento, red, gestión de datos e hipervisor como mínimo, etc.-) dependerá de si existen vías de comunicación fluida con éste, como un comité conjunto de gestión de incidencias o similar. En cualquier caso, sí deberían incluirse aquellos riesgos de tipo técnico asociados al servicio, y no solo los de gobierno del servicio.

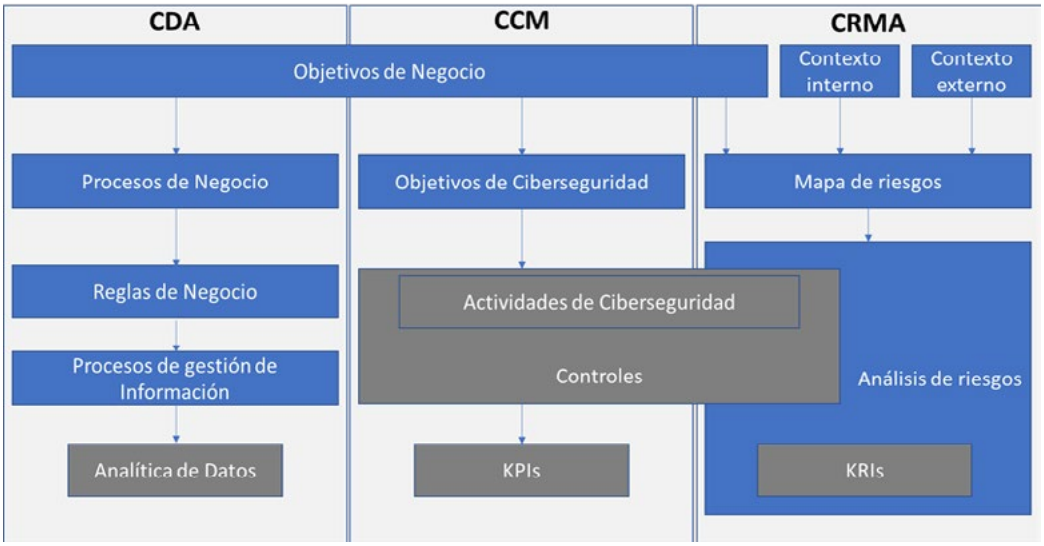
- El reporte que se genere como resultado de este proceso deberá ser comunicado a los órganos de gobierno y control de la organización, pero no al CSP, puesto que en éstos deberá ofrecerse una visión global del riesgo para la organización, y la información relativa al servicio cloud estará representada o agregada junto a otra de tipo interno que no debería ser trasladada al CSP.

- Este proceso debe comprender no solo la monitorización del riesgo mediante la medición y análisis de KRIs, sino también las actividades de respuesta que deban realizarse en caso de que se detecte una situación que deba ser gestionada. Es probable, en la medida en la que este proceso se implante en organizaciones con una madurez elevada en la gestión de los riesgos, que ya exista una estrategia de respuesta a incidentes. En tal caso, deberá asegurarse que ambos procesos se integren, y la información reportada como resultado de la ejecución del proceso se integre con las actividades de gestión y tratamiento de riesgo de la organización.

ELEMENTOS CLAVE 4.

4.1. Dependencias para la definición los elementos clave.

Los elementos incluidos en la presente sección, si bien no pueden considerarse parte del modelo de supervisión desde un punto de vista formal, soportan la definición de los elementos clave de supervisión, y por tanto deben ser tenidos en cuenta.



4.1.1. Objetivos de Negocio.

Los objetivos de negocio representan un aspecto fundamental sobre el que construir la función de ciberseguridad de la organización, y que por tanto deberá ser tenido en cuenta a la hora de definir los elementos subyacentes.

Estos objetivos se obtienen a partir de las necesidades del negocio, en lo que respecta al modelo de negocio, la estrategia de desarrollo, etc., así como a los requerimientos generales impues-

La decisión que lleva a la organización a adoptar servicios en la nube debería partir de estos objetivos, y dar respuesta a una de las necesidades del negocio, habiendo una justificación precisa para su adopción, y una relación clara entre la adopción del servicio y la consecución de uno o más de dichos objetivos.

4.1.2. Contexto interno.

El contexto interno de la organización representa todos aquellos elementos bajo el control de la organización y que impactan tanto en los riesgos a los que ésta se ve expuesta, como en la estrategia y los propios objetivos de ciberseguridad.

Dentro del contexto interno se encontrarán todos los recursos tecnológicos utilizados por la organización, entre los que se incluye el servicio en la nube, así como la infraestructura subyacente a dicho servicio bajo el control de la organización.

4.1.3. Contexto externo.

En contraposición al contexto interno, el contexto externo representa todas aquellas influencias externas a la organización, así como a la función de ciberseguridad, que en este caso podrán ser tanto internas como externas; y que influirán en la organización y operación de la ciberseguridad en la organización.

Atendiendo al servicio cloud, dentro del contexto externo deberá considerarse al CSP, como una parte interesada más para la organización, así como aquellos condicionantes a los que se vea sujeta la organización por el uso de estos servicios, como regulación particular que le aplique y nuevos actores con los que deba interactuar la organización.

4.1.4. Procesos de Negocio.

A partir de los objetivos del negocio, y para dar respuesta a éstos, se diseñan y operan procesos de negocio, que en su conjunto darán como resultado la operación de la cadena de valor de la organización. Por tanto, los procesos de negocio estarán destinados por un lado a aportar valor y a la obtención de beneficios, y por otro a la ejecución de aquellas funciones que permiten que la organización siga funcionando.

El servicio cloud contratado, dará soporte a uno o más procesos de negocio, y por tanto éstos se verán influenciados por las características y requerimientos del servicio cloud, de la misma

manera que el servicio deberá adaptarse y satisfacer las necesidades y requerimientos de los procesos a los que dé soporte.

4.1.5. Reglas de negocio.

Las reglas de negocio determinan, más allá de los objetivos por los que se ejecutan los procesos, los requerimientos y restricciones a la hora de llevar a cabo las actividades de negocio, por lo que su impacto en la gestión del riesgo tecnológico es relativamente limitado en comparación con el resto de los elementos analizados en esta sección.

Las reglas de negocio no deberían verse modificadas por la adopción de servicios en la nube, puesto que los recursos tecnológicos deberían adaptarse a éstas, y no al revés. En todo caso, dependiendo de lo estrictas que resulten las reglas de negocio, podrán llegar a suponer el descarte de un proveedor o modelo de servicio particular.

4.1.6. Procesos de gestión de información.

A partir de los procesos y las reglas de negocio, para asegurar que los recursos tecnológicos soportan a ambos, deben definirse procesos de gestión de información que aseguren que ésta está disponible en las aplicaciones que requieran hacer uso de ella con el formato y cualidades requeridas para la operación de los procesos, y que la modifiquen para dar reflejo y trazabilidad a la ejecución de los procesos de negocio.

En la medida en la que el servicio cloud, como cualquier otro recurso tecnológico, gestiona la información de la organización, los procesos de gestión de información se ven afectados por éste. En concreto, existe un primer impacto derivado de las características particulares de este servicio frente a otros recursos, así como un segundo impacto asociado a la necesidad de comunicar los recursos TI internos con el servicio Cloud.

4.1.6. Procesos de gestión de información.

A partir de los procesos y las reglas de negocio, para asegurar que los recursos tecnológicos soportan a ambos, deben definirse procesos de gestión de información que aseguren que ésta está disponible en las aplicaciones que requieran hacer uso de ella con el formato y cualidades requeridas para la operación de los procesos, y que la modifiquen para dar reflejo y trazabilidad a la ejecución de los procesos de negocio.

En la medida en la que el servicio cloud, como cualquier otro recurso tecnológico, gestiona la información de la organización, los procesos de gestión de información se ven afectados por éste. En concreto, existe un primer impacto derivado de las características particulares de este servicio frente a otros recursos, así como un segundo impacto asociado a la necesidad de comunicar los recursos TI internos con el servicio Cloud.

4.1.7. Objetivos de Ciberseguridad.

El primer paso a la hora de formalizar la función de gobierno de la ciberseguridad es definir objetivos de ciberseguridad que sirvan de guía para el resto de las actividades y que aseguren el alineamiento con los objetivos del negocio.

La adquisición de servicios cloud, como ocurre con los objetivos de negocio, debe responder también a un objetivo de ciberseguridad, y al mismo tiempo permitir su cumplimiento.

4.1.8. Mapa de riesgos.

El mapa de riesgos corporativo, a partir del análisis del contexto interno y externo de la organización, identifica aquellos riesgos a los que ésta se ve expuesta y que considera de mayor importancia a partir de su impacto potencial para la organización y probabilidad de ocurrencia.

El mapa de riesgos corporativo deberá ser actualizado con la introducción de servicios cloud en la arquitectura de SI/TI, para considerar aquellos riesgos a los que tanto ésta como la organización se ve expuesta introducidos o modificados por el uso de recursos en la nube.

A diferencia del resto de elementos dependientes, en la siguiente sección se incluirá el desarrollo de un mapa de riesgos cloud, puesto que es un elemento crítico para la definición de KRIs y resulta complejo identificar referencias desde las que obtener dicho mapa.

4.1.9. Análisis de riesgos.

El proceso de análisis de riesgos es un elemento fundamental que considerar dentro del gobierno de la ciberseguridad, puesto que en él deberían basarse las iniciativas de ciberseguridad desarrolladas por la organización bajo un modelo maduro de gestión. El análisis de riesgos, si bien no tiene por qué verse modificado por los procesos de CA&CM, se integrará tanto para la obtención como para el aporte de información con el proceso de evaluación y monitorización

continua del riesgo. A medida que los procesos de CA&CM evolucionen y adquieran mayor madurez, el nivel de integración podría incrementarse, y la información que fluya bidireccionalmente será mayor.

La modificación con respecto al análisis de riesgos introducida por el uso de servicios cloud se producirá en dos puntos principales. En primer lugar, deberán considerarse los servicios cloud como un recurso tecnológico más a analizar como que formará parte de los activos de la organización. En segundo lugar, como ocurre con el elemento anterior, el análisis de riesgos deberá considerar aquellos riesgos introducidos o modificados por el uso de servicios en la nube.

4.2. Elementos clave.

4.2.1. Analítica de datos.

4.2.1.1. Funciones.

La analítica de datos se usa en diversos procesos de CA&CM. Su función primaria es la de soportar la ejecución del proceso CDA. Sin embargo, también puede ser una herramienta de utilidad para lograr la automatización de los procesos de CRMA y CCM.

A priori, desde un punto de vista conceptual no existen diferencias significativas a la hora de aplicar esta técnica de análisis en un entorno on premise frente a su uso para implementar CA&CM en cloud, puesto que se centra exclusivamente en el análisis de información, y su nivel de independencia sobre la tecnología subyacente es elevado.

No obstante, es importante que la analítica de datos se adapte de forma precisa a los requerimientos de la organización, tanto en lo que respecta a las reglas de negocio a revisar sobre la información, como la implantación del resto de procesos y los servicios cloud contratados.

La mayor diferencia a la hora de ejecutar CDA en cloud frente a usarla para el análisis de recursos on premise radica en las diferencias técnicas a la hora de implementar el proceso de adquisición de información. Sin embargo, el problema de mover datos desde un entorno cloud a un recurso interno resulta trivial, siempre que el servicio permita el acceso a dicho dato.

Las principales funciones de esta técnica a la hora de implementar CA&CM son las siguientes:

4.2.1.1.1. Aseguramiento de la calidad de la información (CDA).

El análisis de datos sustenta el proceso CDA. El objetivo de este proceso es garantizar que no se

producen pérdidas de calidad de la información gestionada. Aunque tradicionalmente CDA se vincula con información de tipología financiera, el análisis de datos como parte del proceso CDA puede realizarse sobre otras tipologías de información, como información operativa de gestión de procesos o sobre los activos tecnológicos y no tecnológicos de la organización, para asegurar su correcta gestión, así como información de control.

Por tanto, la función indispensable del análisis de datos como soporte a CA&CM es la de servir de base al proceso de CDA, y validar la información a lo largo del tiempo, asegurando su coherencia con las reglas de negocio y entre sí. El criterio a la hora de determinar qué información validar dentro de CDA deberá responder a criterios de criticidad e impacto de dicha información para la organización.

4.2.1.1.2. Análisis de tendencias y desviaciones.

Además de la ejecución de análisis estáticos, la analítica de datos es útil para el análisis de la evolución de la información, así como la trazabilidad de la ejecución de procesos sobre ésta. Como otro de los aspectos fundamentales de CDA, la analítica de datos puede utilizar técnicas estadísticas para identificar tendencias y desviaciones en la información y las modificaciones producidas sobre ésta, aportando información de valor para cualquiera de los procesos que forman CA&CM.

4.2.1.1.3. Soporte a la provisión de información para el análisis posterior de los procesos de CA&CM

Además de la ejecución de análisis estáticos, la analítica de datos es útil para el análisis de la evolución de la información, así como la trazabilidad de la ejecución de procesos sobre ésta. Como otro de los aspectos fundamentales de CDA, la analítica de datos puede utilizar técnicas estadísticas para identificar tendencias y desviaciones en la información y las modificaciones producidas sobre ésta, aportando información de valor para cualquiera de los procesos que forman CA&CM.

Esto permitirá optimizar los procesos de adquisición y depuración de información en el propio entorno, de forma que solo se transfiera aquella información que resulte representativa y de calidad, para su posterior análisis.

4.2.1.1.4. Soporte al análisis de controles y riesgos (KPIs y KRIs).

Además de analizar la calidad de la información de valor para la organización y de organizar toda la información generada para su posterior análisis, el análisis de datos puede dar soporte a los procesos CCM y CRMA para analizar de forma rápida un gran volumen de información, lo que resulta necesario para poder analizar de forma continua controles, KPIs y KRIs.

Aunque no es necesario utilizar técnicas de análisis de datos para cubrir los aspectos anteriormente indicados, para poder lograr un alto nivel de automatización e incrementar su frecuencia hasta conseguir un proceso de ejecución continua, debe utilizarse esta técnica o alguna similar, en lugar de recurrir a análisis manuales no automatizados.

4.2.1.2. Fases.

4.2.1.2.1. Planificación.

Antes de iniciar el trabajo de análisis como tal, y solo como parte de la primera iteración, o de aquellas posteriores que requieran cambios en el modelo de análisis fruto de cambios en los requerimientos del negocio o del proceso CDA, debe llevarse a cabo la planificación del análisis que se llevará a cabo posteriormente.

La planificación comienza con un proceso de concienciación al resto de la organización, de forma que se lleve a cabo un levantamiento inicial de la información de todas las áreas de la organización para poder obtener un entendimiento inicial sobre las principales tipologías de datos gestionadas por la casa, el uso que se hace de éstos y su importancia.

Este proceso de planificación inicial debe formalizarse en un programa de gestión de datos, que servirá como documento maestro en el que se identificarán tanto el diccionario de datos completo de la organización, incluyendo tipologías, usos, origen y responsabilidades; como las estrategias que se utilizarán para la medición de la calidad y para el proceso de supervisión posterior.

Cuando la complejidad de la organización sea elevada, también podrá resultar necesario llevar a cabo un proyecto de migración que permitan definir, implantar y poblar la arquitectura TI que dará soporte al proceso de análisis de datos.

4.2.1.2.2. Recopilación de datos.

El objetivo de la recopilación de datos es poblar el modelo de control en el que se sustentan los procesos que forman CA&CM. Existen dos objetivos básicos que deben satisfacerse para lograr una recopilación de datos satisfactoria: (i) obtener información suficiente para validar la calidad de la información alojada en cloud y las reglas de negocio que deberían aplicar sobre ésta, y (ii) adquirir la información mínima requerida para permitir la evaluación de controles, KPIs y KRIs.

Partiendo de la definición de estos elementos básicos para la supervisión, debe definirse un modelo de gobierno de la información que identifique el responsable de cada elemento a recopilar, su localización y una estrategia de adquisición adaptada a las características de cada tipo de dato.

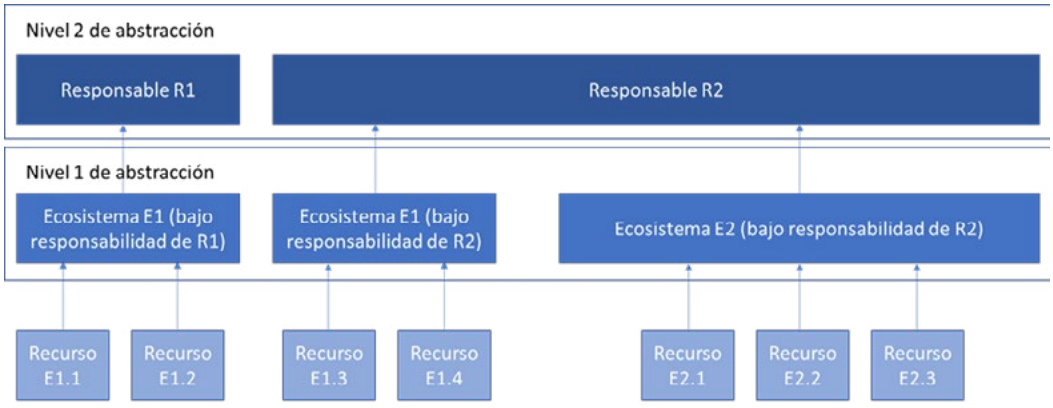
Aunque debe tratarse de automatizar todo lo posible la recopilación de datos, hay determinados elementos que no podrán ser poblados automáticamente.

Hay que tener en cuenta que a pesar de que determinados controles deban ser implantados por el CSP, la responsabilidad de validar que existen niveles de seguridad apropiados para el tratamiento de los datos y ejecución de procesos soportados por el servicio siempre recaerá sobre el cliente, por lo que tendrá que coordinarse con el CSP para la obtención de información que le permitan analizar el nivel de implantación y eficacia de los controles implementados por el CSP.

4.2.1.2.3. Agregación de datos

Dado que el ecosistema tecnológico de una organización que hace uso de servicios cloud es por lo general heterogéneo, una vez obtenidos los datos para una determinada arquitectura de TI en uso, debe procederse a su agregación para poder llevar a cabo un análisis conjunto. Esto incluirá la agregación de datos obtenidos como resultado de la evaluación de los servicios cloud contratados, así como aquellos que reflejen la situación de la arquitectura TI desplegada on premise. Adicionalmente, también podrá resultar necesario incorporar los datos necesarios para la evaluación de la arquitectura de TI de aquellos proveedores que gestionen datos de la organización en sus sistemas.

Puede resultar necesario llevar a cabo la agregación en distintas etapas, dependiendo de la distribución entre las distintas arquitecturas de TI en las que se soportan los procesos de la organización y los actores involucrados en cada una de ella. Para la obtención de resultados más fácilmente interpretables, a la hora de agregar esta información, es recomendable agrupar en alguna de las fases según el actor responsable de implementar controles de seguridad en cada una de las arquitecturas. Una vez realizada la agrupación por actores, la siguiente fase de agrupación debería ofrecer una visión que permita cubrir cada uno de los ecosistemas o arquitecturas de TI de los que haga uso la organización. Es importante que, al pasar de una visión centrada en actores a una centrada en arquitecturas, se deje traza sobre las responsabilidades de cada actor sobre cada uno de los ecosistemas o arquitecturas.



4.2.1.2.4. Validación de datos.

La validación de datos debe llevarse a cabo en cada una de las fases de agregación. Dicha validación debe asegurar por un lado que no hay inconsistencias aparentes en la información recopilada, de forma previa a la agregación. Por otro lado, deberá comparar la información obtenida para cada elemento a analizar, para asegurar que permite la ejecución del análisis posterior, así como la coherencia en su volumen y detalle.

Por ejemplo, podría resultar ineficiente o poco efectiva la obtención de un volumen de información para un entorno SaaS que fuera muy superior al recopilado para un entorno IaaS, dado que la capacidad de control y supervisión en el segundo caso es superior al del primero.

Por otro lado, también debe validarse que la asignación de responsabilidades para la implantación y ejecución de controles se haya distribuido correctamente durante los procesos de agregación, y que el mapeo necesario para dotar de trazabilidad a este proceso sea correcto. Adicionalmente, se validará que el marco de controles y el mapa de amenazas se mantenga consistente a lo largo de todas las arquitecturas o ecosistemas, y que los datos obtenidos permitan evaluarlo de forma completa.

4.2.1.2.5. Análisis de datos.

Se trata de la última fase del proceso, y en ella se ejecutan las validaciones diseñadas por la organización a partir de las reglas de negocio definidas, una vez comprobados que los datos para llevar a cabo dichas validaciones no presentan incidencias aparentes. En los siguientes apartados, se identificarán los objetivos de este proceso y los aspectos a evaluar.

Como parte del análisis de datos, deben llevarse a cabo las siguientes subactividades:

4.2.1.2.5.1. Identificación de reglas de negocio.

El resultado de la ejecución de análisis de análisis de datos debe dar respuesta a las necesidades del negocio, y tener en cuenta sus requerimientos para poder llegar a conclusiones que resulten válidas en el contexto de la organización.

Para lograr que el análisis de datos aporte valor a la organización, las pruebas que se ejecuten deben construirse partiendo de las reglas de negocio que apliquen sobre los distintos procesos, de forma que dichas reglas puedan trasladarse posteriormente a los datos de los que dispone la organización.

En este sentido, a la hora de aplicar esta técnica a un entorno cloud, deberá adquirirse un entendimiento preciso sobre los procesos ejecutados en el entorno cloud y cómo estos modifican tanto la información alojada en dicho entorno como el resto de información a disposición de la organización.

- ***4.2.1.2.5.2. Creación de reglas de calidad sobre los datos.***

Una vez definidas las reglas de negocio, deben identificarse, a partir de éstas, las reglas que aplican sobre la información, de forma que se determinen características mínimas de calidad, valores que puede adoptar cada tipo de dato, reglas relacionales que deban aplicarse sobre dos o más tipologías de datos, cambios permitidos sobre un tipo de dato, etc.

Entender las características de la información y cómo ésta se comporta permitirá definir las pruebas de calidad que tendrán que ejecutarse a intervalos regulares para identificar posibles incidencias y analizar la evolución de la calidad de la información a lo largo del tiempo.

- ***4.2.1.2.5.3. Preparación.***

Aunque esta subactividad puede omitirse a medida que se ejecuten iteraciones del proceso CDA, una vez realizada la primera carga de información validada para su análisis, o cuando se produzcan cambios en los requerimientos de análisis, debe llevarse a cabo la preparación del entorno de análisis.

Esta preparación comprende la carga de datos en el entorno donde se vayan a producir su análisis, incluyendo el formateo de éstos para adaptarlos a la herramienta de análisis utilizada y un análisis inicial ad hoc sobre la información cargada, de forma que ésta se estructure para facilitar su análisis; y permita validar si las pruebas de calidad definidas se podrán ejecutar sobre los datos capturados tal y como se habían diseñado.

- ***4.2.1.2.5.3. Preparación.***

Aunque esta subactividad puede omitirse a medida que se ejecuten iteraciones del proceso CDA, una vez realizada la primera carga de información validada para su análisis, o cuando se produzcan cambios en los requerimientos de análisis, debe llevarse a cabo la preparación del entorno de análisis.

Esta preparación comprende la carga de datos en el entorno donde se vayan a producir su análisis, incluyendo el formateo de éstos para adaptarlos a la herramienta de análisis utilizada y un análisis inicial ad hoc sobre la información cargada, de forma que ésta se estructure para facilitar

su análisis; y permita validar si las pruebas de calidad definidas se podrán ejecutar sobre los datos capturados tal y como se habían diseñado.

4.2.1.2.5.4. Establecimiento de métricas de calidad.

Para conseguir un enfoque de aseguramiento continuo sobre el análisis de datos, y poder integrarlo en el proceso CDA, además de ejecutar las pruebas de calidad de forma periódica, es necesario definir métricas de calidad que permitan entender la evolución de la calidad a lo largo del tiempo, e identificar de forma ágil aquellos datos que no posean la calidad requerida para la correcta ejecución de los procesos de la organización.

La forma de lograr esto es mediante la definición de métricas de calidad que permitan, una vez ejecutadas las pruebas, representar la relación entre los resultados obtenidos y los requerimientos y objetivos de calidad de la información para el negocio. Estas métricas aportarán información que será más fácilmente trasladable al resto de procesos, al ofrecer trazabilidad sobre las incidencias, su origen y los impactos que éstas tienen sobre el negocio.

4.2.1.2.5.5. Análisis de métricas e identificación de desviaciones.

Una vez definidas las métricas, deben ejecutarse pruebas periódicamente que permitan obtener mediciones de dichas métricas a lo largo del tiempo. Estas mediciones deben analizarse tanto de forma estática como agregada, de manera se analicen y traten tanto las mediciones cuyo resultado esté por debajo del nivel objetivo para la métrica correspondiente, como aquellas fluctuaciones o desviaciones que se consideren anómalas o que reflejen una situación perjudicial para el negocio.

4.2.1.2.5.6. Generación automatizada de reportes.

La información agregada sobre las métricas evaluadas a lo largo del tiempo debe usarse para el reporte a los órganos de gobierno y control, así como para nutrir la función de aseguramiento de la organización. En la medida en la que la generación de estos reportes se automatice, la integración del análisis de datos con otros procesos de ejecución continua se podrá realizar de forma más sencilla.

Estos reportes tendrán que adaptarse dependiendo de la finalidad de los mismos. En caso de que deban integrarse con otro proceso automatizado, podría resultar recomendable optar por desagregar la información para que pueda ser analizada en detalle. En cambio, cuando se vayan a usar como reporte final a un área u órgano concreto dentro de la organización, es preferible incrementar el nivel de agregación de la información, y utilizar un enfoque de análisis que dé respuestas a las necesidades e inquietudes de cada interlocutor al que se dirija.

4.2.1.2.6. Refinamiento.

Tratándose de un proceso iterativo, la primera iteración de CDA presentará ciertas deficiencias que será necesario corregir. Inicialmente, pueden existir reglas de negocio que se hayan obviado, y relaciones que no se hayan tenido en cuenta. Una vez finalizada la ejecución de una iteración, es conveniente revisar no solo los resultados obtenidos sino el modelo de supervisión construido, para implementar las mejoras y correcciones que se hayan determinado oportunas en fases previas. Es posible que tras el contraste con las partes interesadas se identifiquen pruebas mal configuradas, o conclusiones erróneas, así como otras reglas relevantes que no se hayan tenido en cuenta.

Esta fase no solo servirá para realizar correcciones sobre el proceso, sino para asegurar que éste se mantiene alineado con los requerimientos del negocio a lo largo del tiempo. Es importante no solo compartir los resultados del análisis con las partes interesadas, sino también obtener feedback de éstas sobre cambios organizativos y operativos, así como sobre el propio proceso de CDA, para favorecer un incremento en el aporte de valor a medida que se ejecuten iteraciones sucesivas.

Como parte de esta fase, también deberá realizarse un proceso de análisis interno que analice posibles mejoras en el proceso, incluyendo la depuración o simplificación de reglas, y la introducción de un grado mayor de automatización sobre el proceso de análisis y reporting.

4.2.1.3. Integración del análisis de datos en la función de aseguramiento.

En lo que respecta a la finalidad del análisis de datos, su uso va más allá del soporte a CDA. La analítica de datos puede ser integrada directamente en la ejecución de auditorías tradicionales, y merece la pena ser considerada incluso de forma aislada a la integración de CA&CM.

La siguiente tabla muestra diversas técnicas analíticas que pueden ser utilizadas durante la ejecución de CA&CM y de auditorías tradicionales:

Fase del análisis en auditoría	Proceso CA&CM soportado	Método analítico	Descripción
Evaluación inicial	Transversal	• Monitorización de fuentes abiertas • Etnografía • Observación • Entrevistas	En esta fase, el auditor debe identificar las características de la organización cliente del servicio cloud, así como los detalles del entorno de control de esta o de cualquier otro actor involucrado en la gestión de datos propiedad de la organización o de los que ésta sea responsable.
Planificación de la auditoría	CRMA	• Análisis de ratios • Grupos focales • Revisión documental • Análisis de desviaciones y tendencias	El objetivo de esta fase es llevar a cabo una identificación inicial del nivel de riesgo al que está expuesta la organización, para poder determinar los aspectos mínimos que deberían revisarse durante las auditorías y aquellos que deberían cubrir los procesos de CA&CM.
Evaluación del riesgo		• Análisis cuantitativo (análisis de datos) • Entrevistas	Esta fase se corresponde de forma directa con el proceso de CRMA, que se sustenta en el análisis de KRIs para el establecimiento de niveles de riesgo, y que será utilizado para poder planificar auditorías que cubran aquellos riesgos de mayor relevancia para la organización.
Evaluación de controles	CCM	• Análisis cuantitativo (análisis de datos) • Entrevistas • Cuestionarios	Esta fase se enmarca en el trabajo de campo en una auditoría convencional, y corresponde al proceso CCM en CA&CM, sustentándose fundamentalmente en el análisis cuantitativo de datos obtenidos sobre el desempeño de los controles implantados.
Análisis de cumplimiento	CDA CRMA CCM	• Análisis cuantitativo (análisis de datos)	El objetivo de esta fase es identificar si los elementos básicos para el control del riesgo tecnológico se encuentran implantados y funcionando, considerando todos los elementos para el control y supervisión de los riesgos.
Pruebas sustantivas	CCM CRMA CCM	• Análisis cuantitativo (análisis de datos)	Cubre la eficacia de las medidas desplegadas para la protección del riesgo, y afecta a todos los procesos de CA&CM, siendo la fase que permite obtener de forma más precisa los resultados y conclusiones esperadas por dichos procesos.
Emisión de conclusiones	CCM CRMA	• Uso de sistemas expertos • Análisis basado en big data • Análisis de patrones	El objetivo de esta fase es obtener conclusiones a partir de grandes volúmenes de datos estructurados y no estructurados, por lo que puede automatizarse usando sistemas especializados en este tipo de análisis y en la toma de decisiones.

Como se ha expuesto anteriormente, el análisis de datos cubre diversos elementos de control del modelo CA&CM, incluyendo la calidad de la información gestionada por la organización, los controles desplegados para la gestión del riesgo y los KPIs y KRIs de desempeño. Sobre estos elementos, la analítica de datos debe procurar lo siguiente:

- Identificación y análisis de patrones anómalos en la información o el funcionamiento de los elementos de control.
- Análisis y visualización del funcionamiento y rendimiento de los elementos de control a lo largo de los distintos procesos, sistemas, y ecosistemas o arquitecturas utilizadas por la organización.
- Establecimiento de modelos estadísticos o predictivos que permitan el análisis y contextualización de los datos obtenidos, la proyección a futuro y la identificación de fluctuaciones en los valores de medición obtenidos que requieran un análisis posterior.
- Favorecer la integración de información procedente de orígenes y análisis heterogéneos para lograr una supervisión consistente a lo largo de todos los recursos tecnológicos utilizados por la organización.

4.2.1.4. Input/output en la analítica de datos.

El análisis de datos es una técnica que deben integrarse dentro de los procesos de CA&CM. Existen diversas actividades que deben llevarse a cabo tanto para nutrir el análisis de datos, como para que éste aporte valor a los procesos que componen CA&CM.

Las principales actividades que deben llevarse a cabo para poder usar el análisis de datos como soporte a estos procesos son las siguientes:

4.2.1.4.1. Obtención de las reglas de negocio a aplicar sobre controles, KPIs y KRIs para su análisis.

El análisis de datos debe tener en cuenta las características y necesidades del negocio para determinar qué información debe preservar su calidad, así como el impacto o criticidad en caso de que cada tipo de información pierda su calidad. Por ello, para poder llevar a cabo un proceso de análisis de datos, el primer paso es entender cómo deben comportarse los controles, KPIs y KRIs, y qué información debe entenderse para entender su comportamiento.

4.2.1.4.2. Traducción de las reglas de negocio en reglas de análisis de datos.

Una vez que se han obtenido las reglas de negocio que deben aplicarse sobre el análisis de controles, KPIs y KRIs, es necesario llevar a cabo una traducción de dichas reglas en reglas que

apliquen sobre la información analizada. Este proceso comprende la traducción de requerimientos de control en requerimientos de bajo nivel sobre la información.

4.2.1.4.3. Identificación de las fuentes de información válidas para el análisis de cada elemento.

Tan importante como contar con los datos apropiados, es conocer la fuente adecuada para obtenerlos. Para que el análisis de datos aporte valor a la organización deben identificarse ambos aspectos, lo que asegurará que se obtenga la información oportuna desde una fuente fiable y representativa para cada control, KPI y KRI a analizar.

4.2.1.4.4. Utilización de la información producto del análisis como input para la ejecución de auditorías.

Una vez que los datos han sido analizados y se han identificado incidencias y desviaciones, éstas deben considerarse para la planificación y diseño de auditorías, dado que en muchos casos será necesario hacer un análisis en profundidad de casos puntuales, para identificar las causas origen de los aspectos relevantes identificados y poder tratarlos cuando así se considere necesario.

4.2.1.4.5. Provisión de información de reporte para el tratamiento posterior de incidencias.

Además de nutrir el proceso de auditoría, el análisis de datos también puede usarse como una herramienta capaz de detectar la causa origen de las incidencias que se produzcan en la organización. Entender la relación y evolución de la información podrá ayudar a detectar el origen de comportamientos no esperados sobre la información de la organización.

4.2.1.4.6. Generación de reportes para los Órganos de Gobierno y Control.

Una vez que el conocimiento generado como resultado de la ejecución de análisis de datos se formatea y sintetiza de forma adecuada, puede ser de mucha utilidad para que los órganos de gobierno y control entiendan la situación de la organización y soportar la toma de decisiones.

4.2.1.5. Dimensiones de calidad.

Cuando el análisis de datos se utilice como medio para implementar CDA, que se centra exclusivamente en la calidad de la información, es importante que las pruebas que se diseñen permitan validar todas las dimensiones que comprenden la calidad de los datos, las cuales se incluyen en la siguiente tabla:

Dimensión	Finalidad
Accesibilidad	La información está disponible para su consulta y puede obtenerse de forma fácil y rápida.
Credibilidad	La información es veraz y correcta.
Completitud	No falta información, y ésta posee un volumen y un nivel de detalle adecuado para soportar el proceso que la usa.
Concisión	Se representa con el nivel de síntesis suficiente para no ser excesiva y permitir que su uso soporte la finalidad para la que fue obtenida.
Consistencia	La información se almacena en un formato que permite ser comparada con información similar, y las reglas que relacionan distintos tipos de dato se mantienen.
Gestionable	La información permite su uso en los procesos para los que fue recabada y dicho uso se produce de forma sencilla.
Íntegra	No existen errores en la información, y ésta es correcta y fiable.
Interoperable	La representación de la información es clara y explícita, en lo que respecta a lenguaje, simbología, formato y unidades.
Objetiva	Se trata de información imparcial y no sesgada.
Relevante	Es aplicable y de utilidad para los procesos que la usan.
Reputada	Se ha obtenido de fuentes de confianza.
Actualizada	La información se encuentra suficientemente actualizada como para que pueda ser utilizada por los procesos oportunos.
Entendible	La información debe poderse interpretar de forma sencilla.
Beneficiosa	La información aporta valor o ventaja competitiva.
Única	No se producen duplicidades de un mismo dato, de forma que la organización gestiona un único origen o fuente para éste, y no lo almacena de forma no controlada.

4.2.1.6. Aspectos clave para la integración.

A la hora de implementar CDA sobre un servicio cloud para el análisis de la calidad de la información gestionada en dicho servicio, deben tenerse en cuenta los siguientes aspectos para asegurar el aporte de valor del proceso y que la integración se lleva a cabo de forma efectiva:

- Identificar la arquitectura informacional con la que debe integrarse (sistema monolítico, DWH, sistema distribuido, sistema cooperativo, etc.) para identificar los requerimientos y restricciones que deberán considerarse sobre el servicio cloud en lo que respecta a la gestión y almacenamiento de información.
- Identificar la relación entre la información gestionada en el servicio y aquella almacenada en arquitectura de SI/TI propia de la organización, con el objetivo de identificar interdependencias y flujos de información.
- Analizar las restricciones impuestas por el modelo de servicio y las cláusulas que gobiernan la relación con el CSP para evaluar en qué medida el cliente podrá actuar sobre los datos almacenados o gestionados en la nube.
- Determinar la capacidad de despliegue de herramientas de recopilación de información y análisis de datos en el entorno cloud, para identificar el punto óptimo de la arquitectura tecnológica en el que desplegar las herramientas necesarias para la implantación de CDA.
- Acotar las reglas de calidad de la información que se utilicen para analizar la información en la nube a los requerimientos del negocio y a las limitaciones de actuación por parte del cliente sobre la infraestructura cloud.

4.2.2. Controles.

El análisis de controles es una de las actividades básicas dentro de los modelos de supervisión. Dentro de los procesos de CA&CM aplicados para la supervisión de entornos cloud, hay que tener en cuenta tanto los controles implementados por el proveedor sobre la infraestructura tecnológica que da soporte al servicio, como los que defina el cliente sobre el propio servicio; especialmente cuando dicho servicio incluya elementos de infraestructura.

Dentro de los procesos de CA&CM, el análisis de controles se integra dentro del proceso de monitorización continua de controles (CCM), aunque su selección e implantación debe realizarse de forma previa a la ejecución de dicho proceso.

Una estrategia de ciberseguridad efectiva requerirá la implantación de controles en todas las capas de la infraestructura para asegurar la protección del servicio. Por tanto, será necesario que tanto el cliente como el proveedor del servicio cooperen para garantizar la seguridad del servicio.

En la medida en la que el cliente tenga el control de más capas de la infraestructura subyacente al servicio, al moverse desde modelos de servicio de tipo SaaS a otros de tipo IaaS, deberá encargarse de la protección de cada capa cuya gestión se le delegue. Sin embargo, como mínimo será responsabilidad del CSP la protección de la capa del hipervisor, así como las subyacentes.

Existen por tanto dos tipologías de controles implantados sobre la infraestructura cloud desde la perspectiva del cliente. En primer lugar, están aquellos implantados por el CSP, cuya visibilidad es reducida, sobre los que no tiene capacidad de gestión, y que en muchos casos le vienen ya impuestos al cliente sin poder intervenir en su selección o configuración. En segundo lugar, están los controles implantados por el propio cliente, que podrá seleccionar y configurar sin que el modelo de servicio suponga una restricción, si bien tendrá que considerar los requerimientos concretos de la infraestructura sobre la que los despliega y las capacidades de la organización para su adquisición, configuración y análisis.

El proceso seguido para su selección e implantación variará dependiendo de a cuál de estas dos tipologías pertenezca el control, así como la fase de la gestión de la relación con el proveedor en la que se seleccionarán e implantarán.

4.2.2.1. Controles en las capas gestionadas por el CSP.

Aunque este tipo de controles los implanta y gestiona el proveedor del servicio, el cliente puede adquirir cierta visibilidad sobre ellos, e incluso requerir al CSP la implantación de un conjunto concreto de controles, si bien esto resultará más complejo que en el caso de los controles que el cliente despliegue por sí mismo.

Dentro de esta categoría de controles, a su vez, existen dos subcategorías. Por un lado, hay controles, generalmente de tipo más técnico, con un impacto directo en la infraestructura que soporta el servicio, y que, de no estar implantados, podrían afectar significativamente al servicio o a su seguridad. Por otro lado, existen controles de tipo organizativo, que, sin impactar directamente sobre la infraestructura, asegurarán un adecuado gobierno o gestión de ésta por parte del proveedor, entre los que se encuentran las políticas o procedimientos de operación y seguridad. La implantación de controles sobre el servicio cloud debería seguir las etapas descritas a continuación.

4.2.2.1.1. Selección.

La selección de aquellos controles que deban ser implantados por el CSP deben cubrir los siguientes aspectos:

- **Organizativos.**

Los controles organizativos están destinados a asegurar que el CSP posee una estructura y capacidad organizativa suficiente para la gestión de los riesgos de sus clientes por el uso de los servicios que éste presta. Asimismo, garantizará la capacitación y asignación de recursos para la ejecución de los procesos que aseguren la gestión del riesgo.

- **Gestión.**

Este tipo de controles garantizan que la gestión de la tecnología, los procesos soportados por ésta, y la gestión del riesgo tecnológico se llevan a cabo de acuerdo con las mejores prácticas del mercado y requerimientos del cliente. Esto favorecerá un incremento en la madurez de los procesos y servirá como una línea de defensa más frente a los riesgos tecnológicos.

- **Técnicos generales.**

Un aspecto básico de la protección de los recursos tecnológicos de la organización es la implantación de controles sobre los recursos tecnológicos sensibles. A pesar de que un CSP preste una tipología muy concreta de servicios, en su mayoría, la tecnología sobre la que éstos se apoyan, no está diseñada de forma específica para soportar este tipo de servicios. Por ello, debe protegerse mediante la implantación de controles técnicos aplicando una estrategia de defensa en profundidad que tenga en cuenta todas las capas de la arquitectura tecnológica.

- **Técnicos específicos.**

Para proteger aquellas capas de uso específico en este tipo de servicios, como son la capa de virtualización o hipervisor, la capa de control y la capa de orquestación del servicio, deben desplegarse controles sobre éstas. Este tipo de controles no se encuentran definidos en todos los marcos de control, puesto que son capas de la arquitectura especialmente diseñadas para este tipo de servicios.

La selección de estos controles debe hacerse de forma previa a la selección de un CSP, una vez que se conozca el tipo de servicio a adquirir y el modelo de provisión del mismo (IaaS, PaaS o SaaS). De esta forma, los controles que éste debe tener implantados debe ser un requisito no funcional más para tener en cuenta durante la fase de lanzamiento de la RFP y el análisis de las ofertas.

Dependiendo del tamaño y nivel de consolidación del proveedor, la capacidad del cliente para exigir la aplicación de controles específicos podrá reducirse. Sin embargo, en cualquier caso, el proveedor deberá poder acreditar la aplicación de un conjunto de controles suficiente como

para garantizar una adecuada gestión del riesgo tecnológico, preferiblemente mediante un medio de reporte que ofrezca información detallada para cada uno de los controles a implantar.

4.2.2.1.2. Implantación.

El requerimiento por parte del cliente con respecto a los controles que el CSP debe implantar debe quedar reflejado en el contrato, debiendo llevar a un anexo el detalle de cada uno de estos controles, o el objetivo de control detallado asociado a éstos, y siendo recomendable especificar el marco de control del que se han extraído, para que el proveedor tenga acceso a un mayor detalle sobre cada uno de ellos. La selección de un marco de control específico del que extraer los controles se detallará en el apartado siguiente, correspondiente a la definición de controles en la capa gestionada por el cliente.

Mediante la firma del contrato, el CSP se comprometerá a implantar o tener ya implantados los controles requeridos. En este punto, la utilidad de haber utilizado un marco de control como base para la selección de los controles a implantar radica en que, en la medida en la que dicho marco de control esté más o menos estandarizado y mapeado con otros marcos de control, es más probable que el CSP ya tenga implantados los controles requeridos, o controles similares. De esta forma, la carga extra impuesta sobre el CSP se reducirá, lo que también supondrá una reducción en el sobrecoste asociado a la implantación y mantenimiento de estos controles.

4.2.2.1.3. Requerimientos adicionales.

- **Responsabilidad sobre la implantación y la gestión.**

Aunque el cliente solicite la implantación de determinados controles al CSP, en ningún caso este requerimiento puede suponer una transferencia de responsabilidad en lo relativo a la implantación de dichos controles, a la gestión de los mismos, o al riesgo gestionado.

- **Visibilidad sobre los controles implantados.**

Una vez que el cliente y el CSP acuerden mediante la firma del contrato el conjunto de controles que el proveedor deberá mantener implantados, el cliente debe tener visibilidad sobre dichos controles, desde un punto de vista de su diseño, para conocer cómo se han trasladado los requerimientos incluidos en el contrato. Además, conocer de antemano cómo se han diseñado los controles permitirá saber si cumplen los objetivos de control, y ayudará a realizar una supervisión más eficiente de éstos.

- **Evidencias periódicas de su correcto funcionamiento.**

Tan importante como tener un conjunto de controles suficiente y adecuado para salvaguardar

el servicio, es saber si funcionan correctamente, tal y como fueron diseñados. Para ello, el proveedor deberá facilitar una evidencia periódica de su correcto funcionamiento. Aunque en este punto es habitual que el proveedor recurra a certificados en vigor para acreditar dicho funcionamiento, éstos no aportan suficiente nivel de detalle como para que el cliente pueda conocer qué controles funcionan correctamente y sobre cuáles hay salvedades que tratar. Por tanto, es necesario que se acuerden contractualmente las estructuras de reporting que el CSP pondrá a disposición del cliente para informarle sobre la situación de los controles implantados.

- **Capacidad de supervisión.**

Además de aportar información sobre los controles implantados, para garantizar que éstos cubren los objetivos de control correspondientes y que no existen incidencias sobre éstos que puedan provocar la materialización de un riesgo, la organización usuaria de servicios cloud debe poder supervisar estos controles, tanto mediante la ejecución de auditorías de TI tradicionales, como mediante las actividades de supervisión cubiertas por los procesos de CA&CM. Esta capacidad también debe detallarse en el contrato con el CSP.

4.2.2.2. Controles en las capas gestionadas por el cliente.

A diferencia de lo que ocurre en las capas de la infraestructura tecnológica controladas enteramente por el proveedor, el cliente del servicio puede implantar controles en aquellas capas que controle, especialmente cuando el modelo de servicio permita su gestión, como ocurre en los modelos IaaS. Por otro lado, también es conveniente implantar controles adicionales en la infraestructura tecnológica interna del cliente que se use como punto de conexión o acceso al servicio en la nube.

Esta tipología de controles, aunque deberá tener en cuenta los requerimientos y capacidades del entorno cloud utilizado para la provisión del servicio, no tienen por qué estar especialmente diseñados para su implantación en la nube, puesto que la capa de virtualización ofrece un nivel de abstracción suficiente como para que las capas superiores sean desde un punto de vista funcional y técnico similares a las que podría encontrarse en una infraestructura desplegada on premise.

Los pasos a seguir para la implantación de controles en la arquitectura TI controlada por el siguiente son los siguientes:

4.2.2.2.1. Selección de un marco de control.

El primer paso para seleccionar los controles que se implantarán para salvaguardar el servicio cloud y asegurar una adecuada protección frente al riesgo es elegir un marco de control.

Con respecto al marco de control a seleccionar, puede utilizarse un marco de control generalista para posteriormente adaptarlo a las características del entorno, teniendo en cuenta el uso que la organización hace de éste; o utilizar un marco de control que ya tenga en cuenta controles específicamente diseñados para su despliegue en la nube.

En el caso de los marcos de control que se utilicen para identificar aquellos controles que deberá desplegar el proveedor, es importante que éstos sí tengan en cuenta de manera explícita los recursos y características de la nube, puesto que las capas de la infraestructura en las que se desplegarán son las más diferenciadas con el resto de las arquitecturas tecnológicas, y por tanto deben estar especialmente diseñados para éstas.

Sin embargo, el marco de control utilizado para seleccionar los controles que implementará el propio cliente puede ser más generalista, puesto que se desplegarán sobre capas más homogéneas a lo largo de las distintas arquitecturas. Lo que sí resulta importante es que el marco de control comprenda los usos del servicio y características de la organización, para que todas las actividades desarrolladas y funcionalidades prestadas queden convenientemente protegidas.

Un aspecto clave a la hora de elegir un marco de control aplicable sobre el servicio cloud es que éste esté adecuadamente mapeado con otros marcos de control aceptados por la industria, para asegurar la mejor integración entre los controles desplegados para salvaguardar el servicio y el resto de los controles implementados, tanto del cliente como del CSP. Aunque pueda parecer poco relevante, dado que los procesos de auditoría y monitorización continua se aplicarán sobre el mayor número posible de recursos tecnológicos, y que las mediciones y análisis de controles, y especialmente KPIs, deben aportar resultados consistentes que permitan optimizar un recurso frente a otro, es necesario que se pueda establecer una relación clara entre todos los KPIs analizados que cubran una misma tipología u objetivo de control.

■ *4.2.2.2.1.1. Marcos de controles específicos.*

Estos marcos de controles, entre los que se incluyen la Matriz de Controles Cloud de CSA (CCM, por sus siglas en inglés), o la Norma ISO/IEC 27017, de controles de seguridad para servicios cloud; están especialmente adaptados a este tipo de servicios y a la infraestructura subyacente que les da soporte.

La principal ventaja de optar por este tipo de marco de controles es que requerirán de poca adaptación para su aplicación al servicio cloud, lo que reducirá el nivel de experiencia y recursos requeridos para su aplicación, y favorecerá una correcta interpretación de los objetivos de control asociados.

Sin embargo, puesto que suelen centrarse en la salvaguarda del servicio, como su principal desventaja se encuentra el hecho de que serán más difíciles de mapear con el resto de los controles desplegados por el cliente, lo que podría impactar de forma adversa en la medición de KPIs y el proceso de CRMA.

4.2.2.2.1.2. Marcos de controles generalistas.

Frente a los anteriores, esta tipología de marcos de controles, de tipo más generalista, entre los que se incluyen aquellos definidos en la ISO/IEC 27002, o los de la publicación NIST SP 800-53, ofrecen un enfoque con un mayor nivel de abstracción sobre la infraestructura y servicios cloud. Por tanto, si bien resultarán más complejos de adaptar al servicio cloud, será más fácil asegurar la coherencia entre los resultados de su análisis una vez implantados sobre dicho servicio y aquellos obtenidos como resultado de su evaluación en el resto de los entornos corporativos.

4.2.2.2.1.3. Estrategia de selección del marco de control.

A la hora de optar por una tipología de marco de control específica, uno de los criterios que va a facilitar su selección, es tipo de recurso tecnológico sobre el que se implementará. Si se trata de recursos tecnológicos propios, es preferible optar por un marco de control generalista, que ofrezca un aseguramiento mínimo a todos los elementos de la infraestructura por igual.

Asimismo, para proteger el servicio en la nube, el marco de control generalista puede complementarse con un marco de control específico. De la misma manera, en caso de que la organización haga uso de otra tecnología con características muy determinantes para soportar alguno de sus procesos críticos, sería bueno identificar el marco de controles que mejor le aplique y adoptarlo. En este último caso, aunque no será habitual que exista un marco de control independiente para cada tecnología desarrollada, sí es posible identificar aquel que mejor se adapte a sus características. Por tanto, en este paso, para la selección del marco de control para proteger el servicio, será preferible un marco específicamente diseñado para servicios cloud, como CCM.

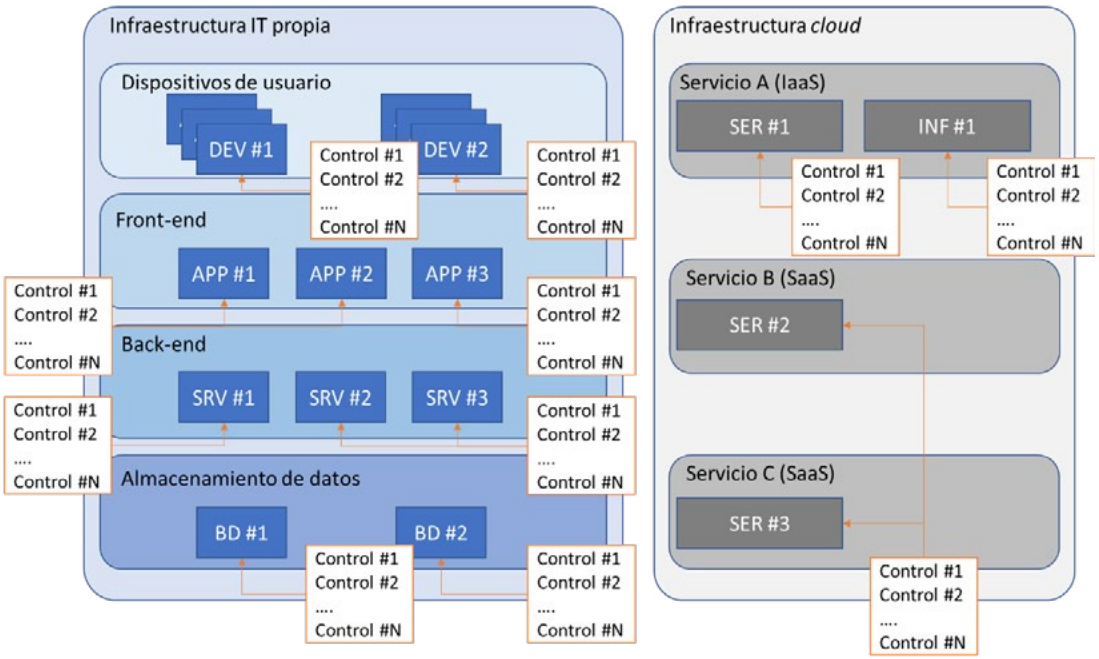
En caso de que la madurez de la organización fuera tan baja que la complejidad de integrar en las siguientes etapas el marco de control específico con el marco de controles generalista no resultase abordable, podría plantearse la posibilidad de implantar sobre el servicio cloud un marco de controles generalista. Sin embargo, incluso en este caso sería preferible optar por marco de control específico, que posteriormente no se integrara con el de la organización, dado que es preferible un adecuado control del riesgo tecnológico, que alcanzar un nivel de madurez en el gobierno de la ciberseguridad mayor.

4.2.2.2.2. Integración del "marco de control cloud" con el resto de los controles.

Una vez que se dispone de un marco de control cuya aplicación se restringe al servicio cloud, y que incluye tanto aquellos elementos de la infraestructura del cliente como del proveedor, es importante integrar dicho marco de control junto con el resto de los controles definidos en la organización para tratar el riesgo tecnológico.

Dado que en las siguientes fases el objetivo es definir KPIs con los que analizar el desempeño de los controles implantados, es importante que los resultados de la medición de estos KPIs ofrezcan una visión coherente a lo largo de toda la organización. En caso de que solo se implementara CA&CM sobre el servicio cloud, se obtendría una visión parcial y sesgada sobre el desempeño de los controles.

Además, es recomendable elaborar un mapa visual de controles, a partir del mapa de arquitectura de SI/TI, en el que se ofrezca una representación gráfica de los controles implantados sobre dicha arquitectura.



Este mapa de controles puede complementarse, en el caso de las arquitecturas de seguridad de la información más complejas, con una matriz de controles, en el que figure cada uno de los controles, junto a su descripción, y los sistemas y procesos sobre los que se encuentran implementados. El desarrollo de este mapa facilitará la labor de consolidación de KPIs que se llevará a cabo durante las fases de reporte.

Controles	Descripción	Recurso A	...	Recurso N
Control A	Descripción general del control A	Especificaciones sobre recurso A		Especificaciones sobre recurso N
Control B				
...				
Control M				

El objetivo de esta matriz de controles es servir de input al proceso de definición de KPIs que se desarrollará en las siguientes fases, y que permitirá alinear los KPIs a los objetivos de control y a las características de los sistemas y procesos.

En el caso de los servicios cloud, se considerará como un sistema más, que dará soporte a determinados procesos ejecutados por el cliente de dichos servicios.

4.2.2.3. Evaluación de controles.

Debe llevarse a cabo la evaluación de controles mediante pruebas de auditoría que permitan validar su eficacia. Para ello, deben diseñarse pruebas de auditoría que cubran los siguientes requerimientos:

4.2.2.3.1. Centrado en el análisis de la eficacia.

Aunque durante la ejecución de auditorías tradicionales el análisis de controles cubra la suficiencia del entorno de control, el diseño particular de cada uno de los controles y la idoneidad de éste para alcanzar el objetivo de control correspondiente, y la eficacia del control, los procesos de CA&CM deben centrarse exclusivamente en el análisis de la eficacia.

Esto se debe a que un aspecto clave del modelo es que las evaluaciones de elementos clave de supervisión estén automatizadas todo lo posible, y que su ejecución se lleve a cabo de forma periódica. Sin embargo, la suficiencia y diseño de los controles no requiere una evaluación periódica, y su automatización es mucho más compleja, llegando a ser impracticable para determinados controles.

La mejor alternativa para plantear una evaluación de controles que se beneficie de una ejecución repetitiva y automatizada consiste en la verificación del funcionamiento de dichos controles, para garantizar que éstos están operando correctamente, y que respetan los requerimientos de diseño.

Aunque se omita la evaluación de la suficiencia y el diseño de los controles de los procesos de evaluación de CA&CM, no quiere decir que estos aspectos no sean importantes, pero su evaluación deberá producirse de forma puntual, cuando se despliegue un control o un nuevo sistema por primera vez, y cuando se produzcan cambios sobre el entorno de control. También deberá evaluarse la suficiencia de los controles y su diseño cuando se lleven a cabo auditorías como actividad complementaria a CA&CM.

4.2.2.3.2. Considerar objetivos de control que abstraigan los detalles técnicos.

El análisis de los controles dentro de CA&CM debe aportar información sobre el funcionamiento de éstos, y sobre si están satisfaciendo los objetivos de control asociados a éstos. No obstante, no debe trascender en el reporte un volumen excesivo de información sobre su operación.

Centrar las conclusiones sobre la eficacia de los controles en el nivel de cumplimiento con los objetivos de control permite aportar una visión mucho más clara sobre si éstos están permitiendo tratar los riesgos o no, y favorece la abstracción de la infraestructura tecnológica, lo que permitirá llevar a cabo reportes consistentes sobre el funcionamiento de controles que cubran un mismo objetivo de control sobre recursos tecnológicos heterogéneos.

Aunque pueda parecer recomendable aportar el mayor volumen posible de información sobre la situación de un control, la incorporación de detalles técnicos sobre la operativa de un control no es necesaria de cara al reporte, aunque pueda ser de utilidad durante el análisis o para la toma de decisiones relativas a su corrección. La forma de lograr un reporte más claro sin que ello entrañe una pérdida de trazabilidad es mediante el establecimiento de estructuras de reporte en las que se puedan trazar todos los análisis llevados a cabo hasta obtener una conclusión depurada.

4.2.2.3.3. Repetibles de forma consistente.

Para dar soporte a un proceso de ejecución periódica, las pruebas que se diseñen deben poderse re-ejecutar a lo largo del tiempo. Más allá del uso de la automatización para lograr esto, las pruebas deben diseñarse para que resulten eficientes, tanto en lo que respecta al volumen de información requerida, como al coste de su ejecución.

Dado que no todas las pruebas serán automatizables, cuando se detecte una que no lo sea, debe someterse a un proceso de evaluación y de identificación de alternativas, para tratar de conseguir una conclusión sobre el mismo objetivo de control de forma automatizable. En caso de no ser posible, debe evaluarse la mejor forma de desarrollar una prueba costo-efectiva a lo largo del tiempo, teniendo en cuenta que el incremento de recursos necesarios a medida que

aumenta el número de pruebas no automatizadas es mucho mayor que en el caso de las automatizadas.

4.2.2.3.4. Hacer uso de la automatización para la evaluación.

El primer objetivo a la hora de diseñar una prueba que evalúe un determinado control debe consistir en asegurar que las conclusiones aportan información relevante sobre su eficacia y el cumplimiento del objetivo de control asociado.

El segundo objetivo debe consistir en conseguir alcanzar un nivel mínimo de automatización en la prueba, para que su re-ejecución sea lo más sencilla posible y consuma el menor número posible de recursos.

El nivel de automatización en la evaluación de un determinado control no se mantendrá constante a lo largo del tiempo. Es preferible un nivel mínimo de controles evaluados en iteraciones tempranas, aunque eso suponga obtener un nivel menor de automatización, que de otro modo requeriría una inversión mayor de tiempo hasta poder ofrecer los primeros resultados.

A medida que se itere sobre el modelo de supervisión, debe buscarse un incremento en dicha automatización. Esta será una forma natural de poder integrar más elementos clave de supervisión en los procesos de CA&CM sin tener que incrementar el número de recursos.

4.2.2.3.5. Obtención la información de fuentes fiables y automatizables.

Tan importante como conseguir que la ejecución de las pruebas sea eficiente y costo-efectiva, es lograr que la información requerida para poder ejecutar dichas pruebas también lo sea. Para ello debe encontrarse el origen que contenga información con la calidad mínima requerida para ejecutar la prueba, y que al mismo tiempo permita una adquisición automatizada de dicha información.

En ocasiones, esto supondrá renunciar a la fuente con el mejor dato disponible y acudir a una fuente alternativa con un dato de menor calidad, aunque suficiente para la ejecución de la prueba; pero que permita obtener información más fácilmente. En general, a medida que se descienda a capas más bajas de la arquitectura tecnológica y de ciberseguridad, se mejorará la capacidad de obtención de información de forma automatizada. Así, por ejemplo, resultará más fácil analizar información procedente de una extracción directa de Base de Datos que de un informe de dicha Base de Datos, o de un procedimiento en el que se indique cómo configurar los accesos a ésta.

La selección de la mejor fuente de información para obtener un dato, más allá de la calidad de la información y la capacidad de automatización de la extracción, también debe tener en cuenta la criticidad del control dentro de la arquitectura de TI y de ciberseguridad, y de la relevancia y características del recurso. Esta información permitirá analizar si resulta viable obtener información de una fuente con una calidad inferior a la mejor disponible a costa de perder precisión en la prueba.

4.2.3. Actividades de Ciberseguridad.

4.2.3.1. Gestión de la infraestructura del cliente.

De acuerdo con las actividades principales de gestión de ciberseguridad descritas en el marco de trabajo publicado por el NIST para la mejora de la ciberseguridad de infraestructuras críticas, deben definirse KPIs para cubrir los grupos de actividades que se detallará a continuación.

De forma similar a como ocurre con los controles, las actividades de ciberseguridad también deberán ser evaluadas. En este caso, el nivel de automatización posible para la evaluación podrá verse reducido, por requerir el análisis de información no estructurada y con formatos homogéneos. Por tanto, aunque el análisis de las actividades de ciberseguridad dentro de CA&CM permita obtener visibilidad sobre la gestión y el gobierno de la organización con respecto a los servicios cloud y resto de infraestructura tecnológica, deberá limitarse dicho análisis para que el consumo de recursos, cuando la supervisión no sea automatizable, no sea excesivo.

Dependiendo del tipo de servicio cloud, estas actividades deberán implementarse también sobre la infraestructura cloud controlada por el cliente.

4.2.3.1.1. Identificar.

- Cubre el análisis del contexto interno y externo de la organización, así como de los recursos destinados a la gestión de la ciberseguridad, como punto de partida para la priorización de los recursos disponibles de forma consistente con los requerimiento y necesidades de la organización y de la función de ciberseguridad.

- El cambio principal introducido en este grupo de actividades a causa del uso de servicios cloud consiste en la consideración de los riesgos introducidos por la adopción del propio servicio, y las particularidades tanto del servicio como del cliente, que introducirán modificaciones en el contexto de la organización.

- Este grupo se subdivide en los siguientes, para los que habrá que asegurar la definición de KPIs:

  - Gestión de activos
  - Contexto del negocio
  - Gobierno
  - Evaluación del riesgo
  - Gestión del riesgo

4.2.3.1.2. Proteger.

- Se focaliza en la protección de la organización frente a los riesgos previamente identificados y evaluados, para asegurar que dicho riesgo se mantiene dentro de los umbrales aceptables.

- Para garantizar la protección de todos los recursos, incluyendo aquellos que se encuentran desplegados en la nube y sobre los que el cliente tiene capacidad de gestión, deberán implantarse controles también sobre las capas de la infraestructura cloud a las que tenga acceso.

- En esta categoría se integrarán los KPIs asociados a la implantación y operación de controles, por lo que siempre que el marco de controles seleccionado sea completo, no será necesario definir KPIs adicionales.

4.2.3.1.3. Detectar.

- De forma complementaria a la implantación de controles de detección, cubiertos en su mayoría en el grupo previo, también es necesario definir KPIs para analizar aquellas actividades destinadas a asegurar una capacidad de detección continua y permanente en caso de que se materialicen riesgos tecnológicos con impacto en la ciberseguridad.

- Es importante, puesto que se produce una pérdida de visibilidad del cliente sobre la infraestructura en la nube, que existan vías de comunicación y coordinación entre el cliente y el CSP para asegurar que el cliente es informado en caso de materialización de riesgos sobre la infraestructura cloud, y por tanto deberán definirse KPIs prar cubrir dicha comunicación coordinada.

- Las subactividades para las que habrá que definir KPIs dentro de este grupo son las siguientes:
  - Gestión de anomalías y eventos
  - Monitorización continua de seguridad
  - Procesos de detección

4.2.3.1.4. Responder.

- También deben definirse KPIs que ofrezcan mediciones sobre la capacidad de la organización para dar respuesta a los riesgos materializados que hayan sido previamente detectados, con la finalidad de evaluar en qué medida se está gestionando los impactos asociados al riesgo materializado.

- De la misma manera que ocurre con la capacidad de detección y los KPIs asociados a ésta cuando se hace uso de servicios cloud, la capacidad de respuesta también debe comprender tanto la dimensión del cliente, como la del proveedor del servicio cloud, en lo que respecta a una respuesta efectiva frente a los riesgos materializados.

- Deberán definirse KPIs para cubrir cada una de las siguientes categorías:
  - Planificación de la capacidad de respuesta
  - Capacidad de comunicación durante la gestión
  - Análisis de riesgos materializados / eventos de seguridad
  - Mitigación de riesgos materializados / eventos de seguridad
  - o Capacidad de reacción y mejora del proceso de respuest

4.2.3.1.5. Recuperar.

- El último grupo de KPIs de actividades de ciberseguridad se destinará a identificar la capacidad con la que la organización y los recursos tecnológicos usados por ésta puede recuperarse tras la materialización de un riesgo de seguridad.

- La recuperación de la infraestructura debe tener en cuenta aquellas actividades que deban ejecutarse sobre el servicio en la nube. Aunque podría parecer que todo el esfuerzo en este caso debería recaer en el CSP, debe analizarse mediante KPIs la capacidad del cliente de adaptar su infraestructura y procesos de gestión del servicio y el CSP para incrementar su resiliencia en caso de que un riesgo similar se vuelva a materializar.

- Los KPIs dentro de este grupo deberán cubrir las siguientes subactividades:
  - Planificación de la Recuperación.
  - Introducción de mejoras o correcciones en la organización y los SI/TI
  - Comunicación durante el proceso de recuperación.

4.2.3.2. Gestión del servicio / infraestructura cloud.

Tal y como se definen en el Estándar NIST SP 500-299, en el que se expone la arquitectura de seguridad de referencia para servicios cloud, existen 4 actividades de seguridad básicas a la hora de garantizar, desde la perspectiva del cliente, la seguridad del servicio en la nube. Sobre estas 4 categorías de actividades deberán definirse KPIs que permitan evaluar su desempeño.

4.2.3.2.1. Soporte al negocio:

- Este conjunto de actividades cubre el gobierno de la relación con el proveedor, para garantizar que haya una comunicación fluida con todas las partes interesadas involucradas en el servicio y que se tienen en cuenta las necesidades del negocio como parte de la gestión del servicio cloud.

- Entre las subactividades que comprenderá este grupo de actividades se encuentran las siguientes:
  - Gestionar la relación con el CSP y coordinar la comunicación con éste.
  - Dar seguimiento a las necesidades y problemas del negocio que tengan impacto o estén causadas por el servicio cloud.
  - Gestionar el ciclo de vida del contrato con el CSP, incluyendo no solo la selección del proveedor y negociación de las cláusulas, sino también asegurando el cumplimiento de éstas a lo largo del tiempo y gestionando los pagos al CSP.
  - Asegurar que el cumplimiento por parte del CSP de los requerimientos de seguridad del cliente es un prerrequisito para la provisión y uso del servicio en la nube.

4.2.3.2.2. Configuración segura.

- La configuración segura del entorno cloud por parte del cliente comprende todas aquellas actividades destinadas a adecuarlo a los requerimientos tanto internos como externos, influenciados por el cuerpo normativo de la organización, estándares de seguridad aplicados o requerimientos regulatorios.

- Las subactividades que deberán gestionarse dentro de este grupo son las siguientes:
  - Garantizar que el aprovisionamiento (despliegue o cambio) de recursos cloud, no solo se realiza de manera eficiente, sino que se realiza de forma segura, tanto en lo que respecta al servicio como a la solicitud de recursos.
  - Supervisar y controlar los recursos desplegados en la nube y los eventos que se produzcan sobre éstos, para garantizar la generación de reportes operativos y de seguridad sobre el servicio.
  - Para asegurar la medición posterior de métricas e indicadores, deben desarrollarse las capacidades necesarias sobre los recursos cloud controlados por el cliente para asegurar la definición de métricas sobre todos los componentes de la infraestructura cloud.
  - Llevar a cabo una adecuada gestión de los acuerdos de nivel de servicio (SLAs) favorecerá el cumplimiento continuo de los requerimientos contractuales, no solo desde un punto de vista operativo, sino también de seguridad y privacidad.

4.2.3.2.3. Portabilidad/Interoperabilidad:

- Este conjunto de actividades está destinado a asegurar que la información, los procesos de gestión de ésta, y los procesos operativos gestionados en sistemas y aplicaciones desplegadas en la nube pueden desplegarse y gestionarse en distintos ecosistemas tecnológicos, tanto si hacen uso de recursos en la nube como si no.

- Deberá controlarse dentro de este grupo al menos lo siguiente:
  - Uso de protocolos, interfaces y sistemas estandarizados, que permiten una interacción sencilla y fluida con otros elementos de la arquitectura de SI/TI que se deban comunicar con el servicio.
  - Uso de lenguajes de programación que favorezcan la portabilidad y reusabilidad del código, cuando se integre en la infraestructura cloud software desarrollado para complementar las funcionalidades básicas ofrecidas.
  - Gestión programada y acotada de cortes por mantenimiento y ante indisponibilidad del servicio para garantizar la integración continua con el resto de la infraestructura de SI/TI de la organización.

4.2.3.2.4. Soporte a la organización.

- Además del soporte al negocio, debe asegurarse una correcta interacción entre el servicio cloud y los requerimientos no funcionales de las áreas de soporte a la organización, especialmente en lo que respecta a las funciones de aseguramiento.

- Los aspectos cubiertos por este grupo son los siguientes:
  - Asegurar el cumplimiento del servicio cloud con los requerimientos normativos y regulatorios de la organización.
  - Gestionar aquellas labores de supervisión que se lleven a cabo sobre el servicio cuando éstas se desarrollen como parte de la función de Gobierno, Riesgo y Cumplimiento.
  - Gestionar el cumplimiento del servicio cloud con los estándares de seguridad y mejores prácticas aplicables.

4.2.3.2.5. Orquestación del servicio.

- A partir de las capas de la infraestructura cloud que estén bajo la gestión directa del cliente según el modelo de servicio cloud adquirido, debe asegurarse que la operación de dichas capas se realiza de forma segura, y está con los requerimientos del negocio.

- Para garantizar una correcta operación del servicio, deberá tenerse en cuenta lo siguiente:
  - El gobierno de SI/TI integra al servicio cloud, y éste se opera de acuerdo con los requerimientos de gobierno de SI/TI corporativo.
  - El gobierno de ciberseguridad integra al servicio cloud, lo que garantiza que las operaciones de ciberseguridad se desarrollan también sobre las capas de la infraestructura controlada por el cliente.

4.2.3.3. Gestión de la relación con el proveedor.

En lo que respecta al control del cliente sobre aquellas actividades bajo la responsabilidad del proveedor de servicios cloud, el estándar NIST SP 500-299 define las siguientes, a partir de aquellos componentes de arquitectura asignados al CSP, para las que deberán definirse los KPIs correspondientes.

4.2.3.3.1. Protección de las capas gestionadas por el CSP.

- Para asegurar que el uso de un servicio cloud se realiza de forma segura, el cliente deberá controlar no solo aquellas partes de la infraestructura tecnológica asociada bajo su control, sino que además deberá asegurar que el CSP ha implementado controles de seguridad en aquellas capas bajo su gestión y que lleva a cabo las actividades de seguridad oportunas.

- El cliente deberá exigir al proveedor un nivel de seguridad mediante la implantación de controles y ejecución de actividades de seguridad similar al que lleva a cabo internamente, para garantizar que el nivel de riesgo se mantiene en un nivel aceptable.

4.2.3.3.2. Abstracción de recursos y control.

- El cliente del servicio en la nube debe asegurar que el CSP ha implementado un nivel de abstracción suficiente entre la instancia que dicho cliente usa y los recursos físicos y lógicos que soportan dicha instancia, de forma que no pueda haber comunicación directa entre dichos recursos y la instancia, ni entre instancias, aunque éstas estén soportadas por los mismos recursos tecnológicos.

- Adicionalmente, el cliente deberá asegurar que el CSP ha implementado controles de acceso suficientes para garantizar el acceso físico y lógico a los recursos tecnológicos que soportan el servicio ofrecido.

4.2.3.3.3. Gestión de recursos físicos.

- Es importante que el control del cliente sobre la infraestructura del CSP que da soporte al servicio cubra adecuadamente los recursos físicos utilizados para ello, incluyendo las instalaciones de procesamiento, hardware de procesamiento, hardware de red y recursos de almacenamiento, de forma que su gestión y despliegue se realice de forma segura y de cumplimiento a los requerimientos del cliente.

4.2.3.3.3. Gestión de recursos físicos.

- El cliente del servicio cloud deberá requerir al CSP el cumplimiento con las políticas, estándares y mejores prácticas de seguridad para el despliegue y configuración de los componentes tecnológicos que dan soporte al servicio cloud.

4.2.3.3.5. Portabilidad e Interoperabilidad.

- En paralelo con la capacidad del cliente de favorecer la migración de los datos desde un servicio cloud a otro, o a un recurso desplegado on premise, el CSP también deberá facilitar dicha migración.

- Hay varios aspectos básicos que debe soportar el CSP a este respecto:
  - La existencia de funcionalidades/herramientas de importación/exportación masiva de datos.
  - La puesta a disposición del cliente de interfaces estandarizadas basadas en estándares cuando dichas interfaces no puedan ser implementadas por el cliente, especialmente en las plataformas PaaS y SaaS.
  - El cliente deberá asegurar que el CSP, una vez que se haya migrado toda la información a la infraestructura de un tercero o del propio cliente, elimina todas las instancias e información del cliente en su arquitectura tecnológica.

4.2.3.3.6. Soporte al negocio.

- En lo que respecta al soporte al negocio ofrecido por el CSP, el cliente del servicio deberá asegurar que éste da soporte a los procesos de seguridad cuya operación no puede ser ejecutada por el cliente.

- En concreto, deberá asegurarse:
  - La gestión segura de las cuentas del cliente que accedan a las interfaces de gestión puestas a su disposición por parte del CSP, o a cualquier otro recurso para el que la gestión de usuarios no esté delegada en el cliente.
  - Facilitar la ejecución de los procesos de seguridad ejecutados por el cliente, especialmente en lo que respecta a la supervisión del servicio y la obtención de información de reporte.
  - Gestionar el catálogo de servicios de forma segura.

4.2.4. KPIs.

4.2.4.1. Características de los KPIs definidos.

Como en muchos otros modelos de medición, los KPIs para su integración en CA&CM deben respetar los principios SMART

- S- Specific – Específico: El KPI debe expresar de forma precisa qué es lo que se va a medir, y a ser posible el objetivo de la medición.

- M – Measurable – Medible: Debe poderse ofrecer un valor cuantitativo como resultado de la medición del KPI, de forma que se pueda analizar su evolución a lo largo del tiempo, y compararse entre distintos puntos de medición (en este caso recursos tecnológicos).

- A – Achievable – Alcanzable: Los KPIs deben ofrecer un punto de partida desde el que mejorar, o tomar decisiones, y dicha mejora o toma de decisiones debe reflejarse en los KPIs. Por ello, establecer metas inalcanzables llevará a la frustración y convertirá al KPI en una medición inútil.

- R – Realistic – Realista: Los resultados de la medición deben ofrecer una visión realista que resulte útil para medir la situación actual del elemento medido.

- T – Time bounded – Acotado en el tiempo: Los KPIs debe permitir analizar el cumplimiento de hitos o umbrales en plazos prefijados de tiempo. Para ello, debe llevarse a cabo una medición periódica con la frecuencia necesaria para poder capturar valores que permitan validar la consecución de los objetivos fijados.

Como un requerimiento adicional, los KPIs deben ser representativos. Puesto que se integrarán en un proceso iterativo, es importante que el proceso sea lo más eficiente posible, y para ello debe lograrse que con el menor número posible de KPIs se aporte información suficiente como para que el proceso aporte valor a la organización.

Aunque no en todos los casos será posible llegar a un nivel adecuado dentro de cada uno de los objetivos, éstos deben estar presentes durante la definición de los KPIs, y aproximarse lo máximo posible a ellos. Algunas características, como la acotación en el tiempo podrían variar de forma independiente al KPI, por lo que podría servir como parámetro de ajuste a medida que la organización vaya adquiriendo madurez, o flexibilizarse en caso de que el esfuerzo de llevar a cabo las mediciones no sea costo-efectivo.

Además de los anteriores, fruto de las características de los entornos cloud y de la homogeneidad entre entornos tecnológicos presente en las organizaciones actuales, convendría tener en cuenta otra serie de objetivos auxiliares:

- Concreto: Aunque existe una menor visibilidad sobre los entornos tecnológicos en la nube, y en línea con los objetivos “Específico” y “Medible”, los posibles resultados de la medición deberían ofrecer no solo resultados cuantitativos, sino suficientemente detallados, optando en todo caso por mediciones semicuantitativas cuando la visibilidad sea casi nula.

- Homogéneo: La medición de un KPI debería reflejar una visión que se abstrajera lo suficiente del elemento medido como para permitir la comparación entre dos mediciones de un KPI sobre distintos recursos tecnológicos. Esto no siempre será fácil de conseguir,

y en ocasiones será preferible incrementar el nivel de detalle a costa de perder la capacidad de comparación.

- Relevante: Aunque se trate de una característica obvia, no debe definirse un KPI cuya medición no vaya a aportar información adicional y de utilidad para entender la situación actual de los recursos tecnológicos analizados. Conviene tener este objetivo en mente para asegurar que no se produzca un desperdicio de recursos.

4.2.4.2. Justificación del uso de KPIs para la medición de controles.

Idealmente, el proceso de monitorización continua de controles se debería basar casi exclusivamente en la evaluación de dichos controles. Este proceso, cuando se integra como una de las actividades dentro de la ejecución de auditorías, debería seguir los principios, buenas prácticas y estándares de auditoría internacionalmente aceptados.

Sin embargo, a causa de la mayor dificultad a la hora de obtener información del CSP o del entorno cloud, es necesario utilizar un enfoque intermedio y más ágil, al menos en organizaciones poco maduras o con poca visibilidad. Esta necesidad se ve incrementada aún más si se considera que parte de la infraestructura y los procesos en los que se sustenta el servicio cloud adquirido ni siquiera son visibles por el cliente.

En este contexto, el uso de KPIs puede sustituir el análisis tradicional de controles. Aunque sustituir el análisis tradicional de controles por la medición de KPIs aporta en general menor confort sobre la situación de los sistemas y del riesgo sobre éstos, puede ofrecer información suficiente como para que la función de aseguramiento planifique auditorías de manera más efectiva.

De hecho, la medición y análisis de KPIs no tiene por qué sustituir a la evaluación de controles dentro del proceso de auditoría, puesto que se produciría incluso antes de que ésta se iniciara, y consistiría en un análisis previo inicial, similar al que se lleva a cabo durante la fase de evaluación preliminar durante una auditoría, que facilita el diseño de las pruebas de auditoría y ayuda a concretar el alcance de la revisión.

En casos en los que la visibilidad sobre el servicio sea extremadamente reducida, podría utilizarse este proceso como único elemento de supervisión que procese CCM, si bien debe tenerse en cuenta el nivel de incertidumbre introducido, así como el riesgo de auditoría asumido, lo que puede suponer no solo la existencia de riesgos no identificados, sino una cuantificación incorrecta de los riesgos puestos de manifiesto.

4.2.4.3. Beneficios asociados al uso de KPIs.

- Permiten evaluar el grado de consecución de un objetivo concreto, o en este caso la efectividad de un control para satisfacer su objetivo de control correspondiente.

- Favorecen el alineamiento entre el estado y evolución de un elemento, en este caso un control, y la consecución de los objetivos de negocio, aportando una visión en la que se consideran los controles desde una perspectiva de coste-eficacia.

- Al reportar información sobre la situación actual y su evolución, permite medir el éxito de un control o corrección sobre éstos de forma precisa, por lo que es más fácil detectar y corregir desviaciones.

- La detección de desviaciones que deban introducir una modificación en la estrategia o el proceso se detectan de forma temprana, por lo que son más fácil de resolver y generan un menor impacto adverso.

- El uso de KPIs mejora el alineamiento entre las necesidades de los clientes y el proceso de gestión de la ciberseguridad y supervisión del servicio cloud, adaptando estas actividades a las necesidades cambiantes de éstos.

- Gracias al incremento en la capacidad de adaptación introducida con la medición y análisis de KPIs, se logra un enfoque más adaptado a un entorno tecnológico tan cambiante como el que soporta los servicios cloud.

- Suponen un modelo de representación sencillo sobre los aspectos más relevantes para el negocio.

- Si se diseñan bien, ofrecen información rica y granular, facilitando un análisis preciso de la situación actual y la toma de decisiones.

- Permiten analizar no solo una situación puntual, sino la evolución de la organización a lo largo del tiempo, por lo que resultan útiles para analizar tendencias, respuesta de los equipos a las decisiones adoptadas, etc.

- Si se integran adecuadamente en la cultura organizativa, y se orientan a la representación del grado de consecución y no de fallo, pueden aportan feedback de calidad y útil para los equipos, lo que puede suponer un elemento clave de concienciación.

4.2.4.4. Posibilidad de integración de KPIs en CA&CM en cloud.

Aunque el uso de un modelo de medición y análisis basado en KPIs para dar soporte a los procesos de CA&CM es algo habitual, al integrar servicios en la nube con el resto de la infraestructura tecnológica de la organización surgen ciertas consideraciones que conviene tener en cuenta.

En primer lugar, en la implementación de CA&CM en cloud propuesta, el uso de KPIs no se usa únicamente como input a estos procesos, sino que también complementa, y en el peor de los casos sustituye, el análisis tradicional de controles dentro de la ejecución de auditorías para aquella parte de la infraestructura externalizada en el CSP. En este último caso, aunque no pueda considerarse que la medición llevada a cabo mediante KPIs aporte el mismo nivel de confort, puede interpretarse que el uso de estos elementos al menos aporta algo de información, cuando no es posible implementar otras técnicas de análisis.

En cualquier caso, el cliente del servicio deberá encontrar la manera de incrementar la supervisión, de forma directa o indirecta, de aquellos controles o aspectos cuyos KPIs asociados devuelvan valores fuera de los rangos permitidos. Esto, a su vez, ayudará a optimizar los recursos de supervisión sobre el servicio, que generalmente se encuentran delimitados contractualmente.

En segundo lugar, existe un doble enfoque tecnológico que debe tener en cuenta para que el uso de KPIs resulte efectivo. Al conjunto de recursos tecnológicos propios utilizados en entornos tradicionales, se suma una o varias infraestructuras tecnológicas que darán soporte a uno o más servicios cloud. Considerando la necesidad de priorizar recursos y ofrecer un aseguramiento consistente a toda la organización, es importante que se usen KPIs para medir no solo aspectos del servicio cloud sino también aspectos de la infraestructura propia.

Aunque en este modelo de CA&CM el uso que se hace de KPIs es de primera aproximación al análisis de controles, y en un entorno tradicional el análisis directo del control resultaría a priori más eficiente, es necesario ofrecer una visión homogénea de todos los recursos tecnológicos, tanto propios como externalizados. Si bien la medición y análisis mediante KPIs se hará para toda la infraestructura tecnológica, el enfoque utilizado para abordar su análisis posterior dentro de la función de auditoría interna de TI variará.

Por tanto, la información proporcionada por los KPIs, al menos de partida, como parte de los procesos de CA&CM, debe considerar indistintamente recursos internos y externos, y los indicadores que se definan deberían ser los mismos para ambas infraestructuras. Esta homogeneización provocará cierta pérdida de precisión en el caso del análisis de recursos tecnológicos internos, a

cambio de una visión comparada más realista de todos los recursos tecnológicos a disposición de la organización.

En tercer lugar, como se verá a continuación, si bien las mediciones de controles mediante KPIs no deberían variar, en lo que respecta a la representación de un grado de consecución del objetivo de control, independientemente de si el control se implementa sobre la infraestructura que da soporte al servicio cloud o sobre infraestructura propia, habrá KPIs específicos que considerará las particularidades de cada una de las tecnologías usadas por la organización. Puesto que este documento se centra en tecnologías cloud, se cubrirán particularidades únicamente de servicios cloud, si bien durante la implementación del modelo deberían tenerse en cuenta las particularidades del resto de tecnologías en uso. El objetivo de este enfoque es que no se dejen de tener en cuenta aquellos aspectos particulares de éstos últimos, y que por tanto el enfoque basado en riesgos sea lo más completo posible.

En cuarto y último lugar, y considerando exclusivamente aquellos KPIs asociados al servicio cloud, así como su impacto en la medición del resto, es importante diseñarlos teniendo en cuenta la información a disposición de la organización usuaria del servicio. Aquí, habrá dos fuentes principales de información: la interacción del cliente con el servicio cloud, de la que podrá extraer mediciones del funcionamiento y comportamiento de éste; y la información provista por el proveedor, cuya provisión deberá estar acordada contractualmente.

En caso de que no se pueda medir el KPI asociado a un determinado control implementado sobre la infraestructura cloud, deberá adaptarse su método de medición exclusivamente a las características de la infraestructura interna, lo que generalmente resultará en una medición más precisa; y tener este hecho en cuenta a la hora de analizar los riesgos de la organización, puesto que la falta de información para evaluar un KPI sobre un control o servicio en ningún caso puede asociarse de forma directa con la existencia de una deficiencia en dicho control o servicio.

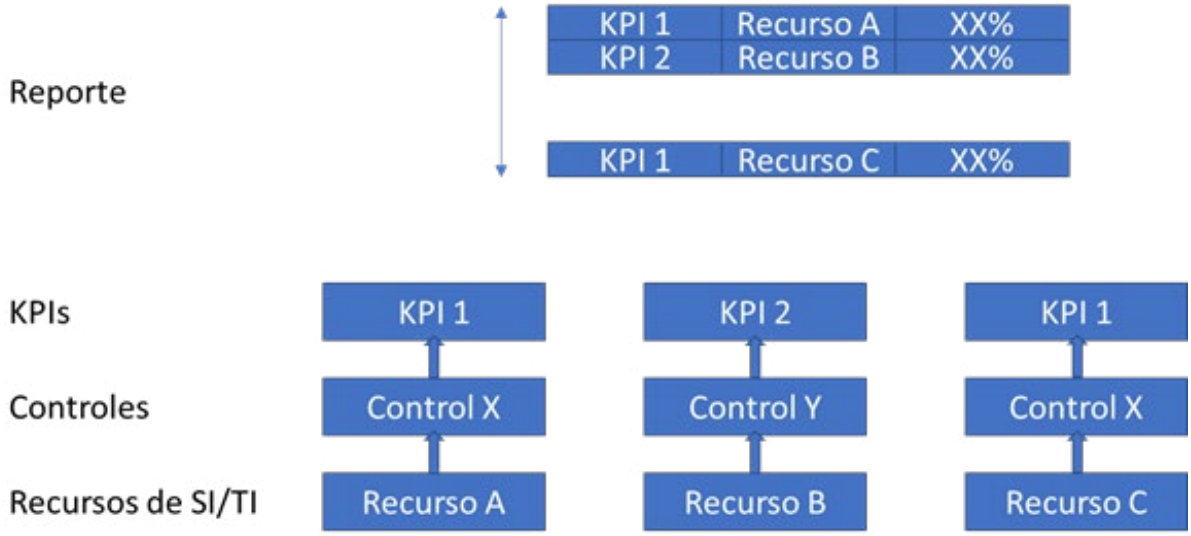
4.2.4.5. Definición de KPIs asociados a los controles implantados (KPIs técnicos).

Para cada uno de los controles incluidos en el mapa de controles elaborado, deberán definirse uno o más KPIs que permitan evaluar su desempeño, ateniendo a las características particulares de cada control y a su objetivo de control asociado.

Para maximizar la utilidad de los KPIs, éstos deben diseñarse de forma que se abstraigan de la implementación particular de los controles, y permitan ofrecer una visión homogénea del cumplimiento de los objetivos de control a lo largo de toda la infraestructura. De esta manera, aunque los controles que formen un determinado dominio de control varíen dependiendo de si se imple-

mentan sobre la infraestructura cloud o si se aplican a nivel interno, los KPIs que se definan deben permitir priorizar los controles implantados sobre cualquier elemento de la infraestructura tecnológica utilizada por el cliente.

Puesto que los recursos de la organización dedicados a la supervisión son limitados, el alcance de la revisión realizada debe basarse en una adecuada priorización de los riesgos de la organización.



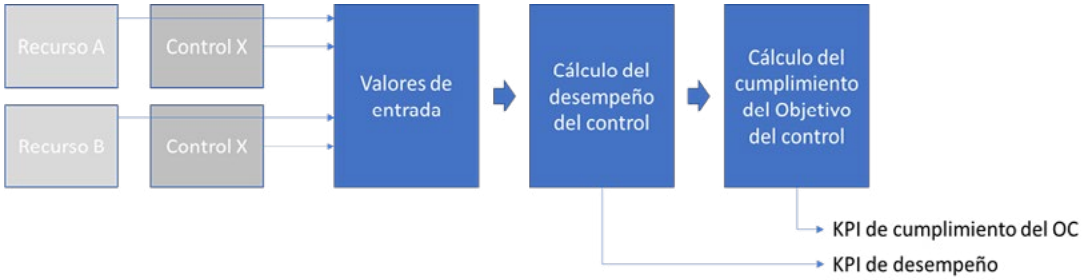
Adicionalmente, para facilitar esta comparativa, es conveniente que los KPIs se basen en mediciones de tipo cuantitativo, para poder priorizar el desempeño de cada uno de los controles implantados sobre cada uno de los recursos sobre los que éste se implementa. El resultado será una matriz de mediciones en las que los ejes serán los controles implantados y los recursos de SI/TI, y en cada celda se incluya el desempeño del control correspondiente sobre un recurso concreto.

La definición de KPIs que permitan obtener una medición de desempeño teniendo en cuenta los recursos y controles analizados, y que aporten el nivel de abstracción requerido para alcanzar resultados priorizables será una de las tareas más complejas a la hora de implantar un proceso de CA&CM, puesto que requiere una alta adaptación a la organización sobre la que se implementa, lo que dificulta el uso de marcos de trabajo y estándares.

A la hora de diseñar estos KPIs, es recomendable considerar en primer lugar los inputs de medición, que será la información generada como resultado de la ejecución de un control concreto implantado sobre un recurso tecnológico específico. Esto permitirá identificar los distintos parámetros a integrar en la fórmula del KPI.

En segundo lugar, una vez que se hayan analizado todos los recursos sobre los que se implanta un mismo control, deberá definirse una fórmula de cálculo que permita ofrecer resultados consistentes entre todas las mediciones. Esta tarea resultará sencilla si el control permite una medición y resultado similares independientemente del recurso sobre el que se implemente, pero irá volviéndose más compleja a medida que en la fórmula deba gestionarse la abstracción necesaria para que frente a implementaciones muy diversas de un mismo control, el resultado mantenga su homogeneidad.

En tercer lugar, sobre una fórmula básica que tenga en cuenta los inputs relevantes para la medición de un control y que permita obtener valores cuantitativos que representen el desempeño del control, deberá introducirse una capa adicional de cálculo que permita representar el cumplimiento del objetivo de control asociado a cada control.



Aunque en última instancia, como input de la función de auditoría y del resto de actividades dentro del proceso de CA&CM, se integrará la medición de más alto nivel para representar el grado de cumplimiento del objetivo de control, es necesario conservar también la medición anterior sobre el desempeño del control, que será de utilidad en caso de que se desee investigar en profundidad una determinada medición, así como para asegurar la trazabilidad del proceso.

4.2.4.6. Definición de KPIs asociados a la estrategia de gestión del servicio cloud (KPIs operativos)

Si bien el objetivo principal de los KPIs es ofrecer una medición comparativa del desempeño de controles, también deben obtenerse mediciones de la gestión de la ciberseguridad realizada por el cliente, utilizando un enfoque que tenga en cuenta todas las capas de gestión de la ciberseguridad en una organización que haga uso de servicios cloud.

4.2.5. Mapa de riesgos

Como requerimiento para la definición, medición y análisis de KRIs, la organización debe tener una visión clara y completa de los riesgos a los que ésta se ve expuesta, de forma que puedan definirse KRIs para el análisis de cada uno de los riesgos identificados. Esta visión se adquiere mediante la definición de un mapa de riesgos que relacione cada recurso tecnológico con las amenazas a las que éstos se ven expuestos.

El mapa de riesgos no se limitará a aquellos que impacten sobre el servicio cloud. Sino que debe cubrir todos los ecosistemas tecnológicos de la organización. A partir del modelado de amenazas y un análisis de los recursos tecnológicos usados por la organización y su criticidad para el negocio e involucración en la provisión de servicios, se establecerá un mapa de riesgos.

De esta manera, se establecerá una relación clara entre cada recurso de la organización, y el nivel de riesgo asociado en caso de que cada una de las amenazas, cuando aplique, impacte sobre dicho recurso. Dado que el tratamiento del riesgo debe realizarse con un enfoque priorizado, el mapa de riesgos será único dentro de la organización, independientemente del número de ecosistemas tecnológicos.

Asimismo, definir un mapa de riesgos asegurará que se defina al menos un KRI para cada uno de los elementos de la matriz, de forma que todos los riesgos se supervisen, y servirá para mantener un punto de referencia global y actualizado sobre la exposición de la organización al riesgo.

4.2.5.1. Proceso para generar un mapa de riesgos.

Los pasos que es necesario seguir para la elaboración de un mapa de riesgos que integre los riesgos a los servicios cloud contratados por la organización son los siguientes:

4.2.5.1.1. Identificación y evaluación de recursos.

La identificación de recursos tecnológicos de la organización comprende en primer lugar el proceso de inventariado de todos aquellos elementos tecnológicos en los que se soporte uno o más procesos de la organización. La identificación de recursos internos, que habitualmente se realiza para la ejecución de los análisis de riesgos tecnológicos de la organización, debe complementarse con la identificación de aquellos que soportan el servicio cloud.

Además de una identificación aislada de elementos tecnológicos, es necesario establecer la relación entre todos ellos, de forma que se expliciten las dependencias existentes y la evaluación posterior de criticidad sea consistente con dichas dependencias.

En el caso de los recursos tecnológicos asociados al servicio en la nube, puede resultar complejo identificar la tecnología subyacente al servicio, a causa de la abstracción de éste de los recur-

sos utilizados para darle soporte. Puesto que el objetivo de este proceso es identificar y en última instancia tratar los riesgos a los que la organización están expuestos, no es necesario llegar al máximo nivel de detalle y profundidad en la identificación.

Para garantizar el tratamiento de los riesgos gestionables por la organización, es imprescindible identificar todos los recursos sobre los que la organización tiene capacidad de decisión o gestión. Asimismo, dado que el cliente es responsable de que el CSP cumpla con las medidas que sean necesarias para que la información del cliente se encuentre correctamente salvaguardada, también será necesario identificar los recursos tecnológicos directamente involucrados en la provisión del servicio, pudiendo obviarse otros recursos adicionales que den soporte a los recursos principales en la provisión del servicio.

Este proceso de identificación de la infraestructura del cliente dependerá en gran medida del acuerdo firmado con el CSP, y de si este contempla la colaboración del CSP en la gestión del riesgo del cliente. Dependiendo de los mecanismos y alcance de la colaboración del CSP con el cliente, deberá adaptarse el proceso de identificación de recursos a las capacidades y visibilidad del cliente sobre el servicio cloud y la infraestructura subyacente. En el peor de los casos, deberá identificarse un único recurso tecnológico asociado al servicio cloud que abstraiga toda la infraestructura tecnológica subyacente a éste, que se usará para cuantificar de forma genérica los riesgos asociados al servicio.

Una vez identificados todos los recursos tecnológicos usados por la organización, el siguiente paso consiste en la cuantificación de la relevancia de ese recurso para la organización. Esta cuantificación, dado que en esta fase aún no se está estimado el impacto asociado a la pérdida, debe basarse en la relevancia del activo para la organización, en términos de involucración en el proceso al que dicho activo soporta, así como a partir de la relevancia de dicho proceso para la organización.

Independientemente de si se realiza una cuantificación cualitativa, cuantitativa, o semicuantitativa, el objetivo de esta etapa es obtener una estimación en la relevancia de cada recurso para la organización desde un punto de vista de negocio, y llevar a cabo una priorización de todos ellos.

Aunque idealmente el resultado de este proceso es obtener una cuantificación precisa de cada activo en términos de importancia para cada uno de los recursos, estableciendo una relación entre los requerimientos de negocio y la necesidad de protección, puede resultar complejo llevar a cabo este proceso de forma estricta. Una forma de relajar este proceso en organizaciones con poco nivel de madurez, o sobre recursos sobre los que no se dispone de suficiente nivel de detalle, consiste en el establecimiento de niveles de relevancia, de forma que cada activo se englobe dentro de una categoría, sin que los recursos de una misma categoría se prioricen entre sí..

En el caso de que no se disponga de información sobre los recursos tecnológicos que soportan el servicio cloud analizado, como alternativa puede basarse la cuantificación de su valor en la importancia del proceso de negocio que soporta dicho servicio, así como en la tipología de datos de la organización que gestiona.

En última instancia, poder establecer una comparación más o menos precisa sobre si un activo es más, menos, o igual de importante que otro para el negocio, es un requerimiento básico para poder continuar con el proceso de establecimiento de un mapa de riesgos.

4.2.5.1.2. Modelado de amenazas

El siguiente paso a la hora de definir un mapa consiste en identificar las principales amenazas a las que se ve expuesto el servicio cloud y la organización en general como resultado de su adopción. La identificación de amenazas, así como la identificación de los puntos de impacto de la organización son por tanto dos elementos esenciales.

Si bien el establecimiento de los riesgos requiere cierto análisis sobre las características de la organización para determinar cuáles son aquellos aspectos que podrían provocar un impacto mayor en caso de ser vulnerados, la identificación de amenazas posee una dimensión más generalista, dado que se basan en el contexto externo, más homogéneo que el contexto interno, y su validez será más fácilmente extrapolable a distintas organizaciones que hagan uso de servicios en la nube.

En general, no existen amenazas que apliquen a un entorno cloud que difieran sustancialmente de aquellas que impactan en recursos tecnológicos desplegados on premise o en otra tipología de recursos tecnológicos externalizados. Sin embargo, es conveniente identificar, a partir de un catálogo generalistas de amenazas, en qué modo y medida impactan sobre servicios en la nube. El modelado de amenazas debe aportar trazabilidad entre los riesgos y los controles necesarios para tratar dichos riesgos. En el Anexo D se detalla el proceso de definición detallada de amenazas para entornos cloud y su relación con los controles incluidos en la Matriz de Controles Cloud de CSA, por ser un marco de control especialmente diseñado para este tipo de entornos.

Como resultado del proceso de modelado de amenazas identificado en dicho Anexo, se han identificado las siguientes amenazas con un impacto relevante en servicios en la nube:

- ***4.2.5.1.2.1. Pérdida de visibilidad sobre el riesgo TI / Fallos en la gestión del riesgo TI .***

Si bien el modelo de computación en la nube se orquesta en torno a servicios, una falta de supervisión de éste por falta del cliente puede llegar a impactar significativamente sobre éste, tanto por una desviación en la calidad o características del servicio, como por la incapacidad del cliente para identificar incumplimientos contractuales en lo que respecta a los requerimientos no funcionales establecidos.

4.2.5.1.2.2. Uso de datos incorrectos.

La falta de gobierno sobre los datos o de controles para garantizar su calidad deriva en una pérdida de calidad de éstos, lo que implica que la organización utiliza información incorrecta tanto como parte de la ejecución de los procesos de negocio, como para la toma de decisiones.

4.2.5.1.2.3. Falta de control sobre los riesgos.

Aunque el cliente del servicio cloud es responsable de garantizar que el uso que hace del servicio se realiza de forma segura, y que éste no supone un incremento en la exposición al riesgo frente al uso de recursos no externalizados, no se llevan a cabo las actividades necesarias para identificar los niveles de seguridad asociados al servicio y asegurar el tratamiento de aquellos riesgos que se encuentren por encima del umbral aceptable.

4.2.5.1.2.4. Incumplimientos regulatorios.

En la medida en la que el servicio cloud soporta procesos de negocio de la organización que los contrata, y almacena datos de los que ésta es responsable, de su uso pueden derivarse incumplimientos de las obligaciones regulatorias de dicha organización, que pueden estar provocados tanto por las características de la infraestructura que da soporte al servicio, como por su propio uso.

4.2.5.1.2.5. Vulneración del servicio.

Un servicio cloud, al ser accedido a través de redes públicas, puede verse expuesto con mayor facilidad a usuarios no autorizados que exploten las vulnerabilidades presentes en éste. De la misma manera, dicha vulneración puede producirse por un usuario que ya tenga acceso al servicio y que haga uso de funcionalidades o acceda a información no autorizadas. Esta vulneración tendrá un carácter generalmente de tipo técnico y provocará el uso de funcionalidades para las que el servicio no fue originalmente concebido.

4.2.5.1.2.6. Protección inadecuada del servicio.

Dado que la infraestructura que da soporte a un servicio cloud puede estar controlada total o parcialmente por el CSP, coordinar la implantación de medidas de seguridad que ofrezcan los niveles de protección que satisfagan las necesidades del cliente puede resultar complejo, y entrañar riesgos en caso de que la protección ofrecida por el CSP no satisfaga las necesidades del cliente.

4.2.5.1.2.7. Uso inadecuado / indebido del servicio.

Una vez que un usuario consiga acceso al servicio, si éste no se encuentra convenientemente protegido, existe la posibilidad de que éste lleve a cabo acciones para las que no ha sido autorizado, haciendo uso de funcionalidades presentes en el servicio a las que no debería tener acceso por su función.

4.2.5.1.2.8. Indisponibilidad de los SI/TI.

Como cualquier otro recurso tecnológico, el servicio cloud puede sufrir pérdidas de disponibilidad, lo que provocará que los procesos soportados por éste no puedan ejecutarse total o parcialmente. Aunque la externalización tecnológica suele estar regulada contractualmente mediante SLAs para garantizar la continuidad del servicio, esto no evita que puedan producirse estas pérdidas, en algunos casos ni siquiera atribuibles al CSP.

4.2.5.1.2.9. Incorrecta gestión de incidentes.

En la medida en la que una incidencia que se produzca sobre el servicio en la nube requerirá la involucración y comunicación entre el CSP y el cliente del servicio, pueden producirse deficiencias en la gestión de incidencias que provoquen que éstas no se resuelvan en tiempo o forma.

4.2.5.1.2.10. Incorrecta gestión de recursos externalizados.

El uso de servicios cloud implica la gestión de diversas capas de la infraestructura tecnológica subyacente por parte del cliente, que podrán verse incrementadas o reducidas dependiendo del modelo de servicio. Dado que dichos recursos no se encuentran físicamente en las instalaciones del cliente y son propiedad del CSP, se introducen complicaciones en su gestión que pueden derivar en impactos operativos o de seguridad para el cliente del servicio.

4.2.5.1.2.11. Pérdida de calidad del servicio.

Aunque un servicio cloud se encuentre accesible, su operativa puede verse degradada por diversos motivos, lo que provocará que, aunque éste se use, no se obtengan los resultados esperados para el negocio, lo que impedirá o dificultará que se consigan los resultados esperados por los procesos que soporta.

4.2.5.1.2.12. Instalación de software malicioso.

Como ocurre en cualquier otro entorno tecnológico, los servicios cloud pueden ser objetivo de infecciones por malware, tanto si la finalidad última de la infección es vulnerar el sistema, o si dicho sistema se utilizará como pivote para una posterior infección o ciberataque.

4.2.5.1.2.13. Falta de gobierno del servicio.

El gobierno del servicio cloud garantiza que éste soporta los objetivos y requerimientos del negocio. En caso de que no se lleve a cabo un correcto gobierno del servicio, pueden producirse diversas situaciones adversas, desde una pérdida de aporte de valor de éste, a su vulneración fruto de una inadecuada protección del mismo. En general, cualquier acción de protección que se lleve a cabo para salvaguardar el servicio sin estar soportada por una estrategia de gobierno adecuada podrá resultar poco efectiva o eficiente.

- ***4.2.5.1.2.14. Acceso físico no autorizado.***

La seguridad física es un componente relevante de cualquier arquitectura de TI. En el caso de los servicios cloud, al soportarse en una arquitectura deslocalizada y utilizada por diversos clientes, existe una pérdida de visibilidad y control por parte de la organización que contrata servicios en la nube sobre el acceso físico a los recursos tecnológicos que dan soporte a dicho servicio, que puede provocar que personas no autorizadas accedan físicamente a la infraestructura física que soporta el servicio sin estar autorizados para ello.

- ***4.2.5.1.2.15. Uso de recursos maliciosos / no autorizados.***

Habitualmente el compromiso de una identidad conlleva el uso indebido de recursos legítimos por parte de un usuario no autorizado. Sin embargo, también puede utilizarse para suplantar la identidad de un recurso tecnológico legítimo, de forma que el servicio cloud o un recurso asociado ilegítimo sea utilizado para fines maliciosos, suplantando el servicio o recurso legítimo.

- ***4.2.5.1.2.16. Pérdida / Fugas de información.***

En cualquiera de los modelos de servicios cloud, se produce el almacenamiento y gestión de información responsabilidad de la organización usuaria de dicho servicio en la infraestructura cloud. Por tanto, un compromiso de dicho servicio o su arquitectura subyacente podrá dar lugar a la exposición de la información sensible de los clientes.

- ***4.2.5.1.2.17. Fraude.***

El servicio cloud, como un recurso tecnológico más, puede ser utilizado por un usuario malicioso para cometer fraude contra la organización que contrata dicho servicio, contra sus usuarios, o contra terceros, valiéndose del servicio o de la identidad suplantada. La organización usuaria del servicio debe prestar atención y protegerse frente a este tipo de amenazas no solo por su posible impacto interno, sino por las consecuencias legales que puede acarrear este tipo de actividad.

- ***4.2.5.1.2.18. Suplantación de identidad de un usuario o un servicio.***

Dado que el acceso al servicio se basa en la identificación de usuarios, una de las amenazas evidentes a las que se ve expuesto éste es el acceso por parte de un usuario malicioso suplantando la identidad de un usuario o servicio legítimo, mediante la vulneración de los medios de autenticación de los que éste haga uso.

- ***4.2.5.1.2.19. Daños provocados por usuarios maliciosos.***

Esta amenaza, muy similar al uso indebido, comprende no solo la ejecución de funcionalidades no permitidas o para las que el usuario no ha sido autorizado, sino también el aprovechamiento de dichas funcionalidades para provocar un perjuicio económico o reputacional a la organización o a las partes interesadas con las que ésta se relaciona.

- ***4.2.5.1.2.20. Fallos en la configuración.***

En la medida en la que la organización que hace uso del servicio cloud tenga capacidad de control o gestión sobre las capas de la infraestructura tecnológica que lo soportan, será responsable de asegurar mediante la configuración de dichas capas que el servicio es seguro, y se alinea con los requerimientos no funcionales de la organización que hace uso de ésta. Un fallo en la configuración provocará que el servicio no se comporte como se esperaba, o que se invaliden total o parcialmente las medidas de seguridad desplegadas para proteger al servicio.

- ***4.2.5.1.2.21. Vendor Lock-in.***

Siempre que se recurre a proveedores para el soporte a procesos de negocio, ya sea desde un punto de vista operativo o tecnológico, existe el riesgo de que la organización se vuelva excesivamente dependiente de dicho proveedor, de forma que no sea capaz de sustituir dicho proveedor por otro o de ejecutar un cambio operativo o tecnológico para prescindir de dicho proveedor.

- ***4.2.5.1.2.22. Pérdida de aporte de valor para la organización / Desaprovechamiento de recursos.***

Aunque los servicios cloud ofrecen por lo general una mayor capacidad de adaptación a los cambios en las necesidades de sus clientes, es posible que se produzca un desaprovechamiento de los recursos de la organización en caso de que el servicio contratado no esté alineado con las necesidades y requerimientos de la organización. Esto puede producirse tanto por una falta de planificación en el momento de la adquisición, como por la ocurrencia de cambios en la organización que no sean tenidos en cuenta a la hora de gestionar dicho servicio o los cambios que deban producirse sobre éste.

- ***4.2.5.1.2.23. Uso indebido o no autorizado de recursos.***

Dependiendo del nivel de acceso que consiga un usuario malicioso, éste podrá no solo hacer un uso indebido del servicio cloud, sino también de los recursos tecnológicos subyacentes a éste, de forma que consiga no solo explotar el servicio, sino hacer uso de la infraestructura tecnológica para sus propios fines.

- ***4.2.5.1.2.24. Fallos en la comunicación.***

Dado que el servicio cloud se comunica con el resto de los ecosistemas tecnológicos de la organización mediante redes públicos, en caso de que haya algún problema con la comunicación entre entornos, se provocará el bloqueo del acceso al servicio.

- ***4.2.5.1.2.25. Incremento no controlado de consumo de recursos.***

Una de las ventajas de los servicios cloud, su elasticidad, puede provocar situaciones adversas para el cliente del servicio. La organización debe ser consciente del modo en el que el servicio escala recursos, puesto que de lo contrario pueden darse situaciones en las que de forma im-

prevista se produzcan incrementos no controlados del consumo, y por tanto de la facturación.

- ***4.2.5.1.2.26. Ciberataques / APTs.***

Los servicios cloud no son inmunes a los ciberataques, tanto si son incidentes puntuales, como si forman parte de un ataque persistente y coordinado, como son las APTs. Estos servicios pueden presentar vulnerabilidades que sean explotadas por atacante para ganar acceso a éstos y llevar a cabo acciones indebidas.

4.2.5.1.3. Cálculo inicial de valores de riesgo.

El cálculo de los valores de riesgo que sirvan como base para la definición de KRIs y para iniciar el proceso CRMA es el siguiente paso una vez identificados los recursos clave de la organización y las principales amenazas a las que éstos se ven expuestos.

Aunque no es estrictamente necesario cuantificar el nivel de riesgo, es una práctica recomendable en un escenario de escasez de recursos. Formalmente, para la definición de los KRIs es suficiente con conocer la relación entre recursos y amenazas. Sin embargo, dado que puede haber una gran disparidad en los riesgos que afectan a la organización, puede incrementarse la eficiencia en el proceso considerando un enfoque dinámico para la definición y medición de KRIs.

Para el establecimiento de una estrategia dinámica, sobre los riesgos cuantificados y priorizados, y tras haber establecido una estructura básica de KRIs que cubra aquellos con mayor afección sobre la organización, debe iniciarse la implantación de aquellos que cubran los riesgos más críticos para la organización, que serán aquellos para los que exista una mayor probabilidad de materialización, o que generen mayores impactos para la organización. Además, estos riesgos podrán ser reforzados mediante la definición de KRIs adicionales. Por tanto, para poder llevar a cabo este proceso de forma eficiente, es preferible realizar un cálculo inicial del riesgo.

Hay que considerar que el cálculo del riesgo para la definición posterior de KRIs no persigue el mismo objetivo que la ejecución de un análisis de riesgos completo y formalizado, puesto que será un input de partida en la primera fase del proceso. Para las siguientes iteraciones, la cuantificación se irá actualizando fruto de la medición y análisis de los propios KRIs.

Bastará por tanto con realizar una estimación del riesgo que permita identificar aquellos recursos y riesgos más relevantes, y establecer una priorización de riesgos y recursos. El objetivo de identificar ambos aspectos es poder ofrecer un nivel de aseguramiento suficiente durante las primeras iteraciones en caso de que no se puedan cubrir todos los riesgos desde la primera iteración del proceso.

4.2.6. KRIs.

La medición de KRIs soporta la evaluación y análisis del riesgo en la misma medida en la que los KPIs permiten la evaluación de controles. En lo que respecta a sus características básicas, éstos deberán respetar los mismos requerimientos expuestos previamente para los KPIs.

Adicionalmente, será necesario tener en cuenta otras consideraciones por las particularidades y finalidad de esta tipología de indicadores.

4.2.6.1. Categorías de indicadores para la gestión del riesgo.

- **Medición de amenazas:** Los KRIs para el análisis de amenazas persiguen la evaluación del nivel de exposición de la organización, considerando tanto amenazas internas como externas.

- **Medición de riesgos:** Esta categoría de KRIs ayuda a establecer la situación de la organización en lo que respecta a los riesgos a los que ésta se ve expuesta, y son los que posteriormente deberán retroalimentar el mapa de riesgos.

- **Medición de cumplimiento:** Como una categoría especial del riesgo TI, estos KRIs servirán para detectar de forma temprana incumplimientos regulatorios.

- **Medición de incidencias:** Otro aspecto relevante dentro de la gestión del riesgo, y para la que se establece esta categoría de KRIs, es la gestión de incidencias, que evalúan la gestión de aquellos riesgos que se materialicen en la organización.

- **Medición del gobierno:** Si bien todas las categorías anteriores ofrecen una visión centrada en el riesgo, esta categoría realiza una evaluación indirecta de éste mediante el análisis de las iniciativas llevadas a cabo en la organización para la gestión del riesgo, incluyendo proyectos internos, certificaciones, etc.

- **Medición de mitigación:** Cada riesgo que supere los umbrales aceptables de la organización debe ser tratado. Por ello, es importante realizar mediciones sobre el tratamiento de los riesgos identificados. A diferencia de la medición de KPIs dentro del proceso de CCM, el objetivo de estas mediciones no es analizar la eficacia de los controles, sino la reducción de los niveles de riesgo hasta límites aceptables.

4.2.6.2. Objetivos para el reporte de KRIs.

El reporte de KRIs debe asegurar criterios mínimos de calidad, incluyendo los siguientes:

- Precisión: Los KRIs deben representar de forma precisa los niveles de riesgo, la capacidad de gestión del riesgo de la organización; de forma que no generen confusión.
- Objetividad: Las mediciones de KRIs y los reportes asociados deben considerar la cultura de riesgo de la organización y utilizar suficiente información como para representar de forma fiel la situación de la organización y su contexto.
- Validez: Las fuentes de información utilizadas para realizar las mediciones de KRIs deben ser fiables y ofrecer información de calidad.
- Relevancia: Los reportes elaborados para presentar las mediciones llevadas a cabo sobre los KRIs deben estar adaptados a la audiencia objetivo y a los procesos en los que se integrará dicha información.
- Completitud: El reporte de KRIs debe comprender todos los ecosistemas tecnológicos de la organización, para ofrecer una visión global del riesgo tecnológico, incluyendo aquellos elementos externos a la organización que influyan en los niveles de riesgo de ésta.
- Actualizado: La información utilizada y las mediciones deben estar actualizadas, de manera que se ofrezca una visión actual del riesgo en la organización.
- Representativo: La cantidad de información incorporada en los reportes debe ser suficiente como para aportar la información requerida por la audiencia y procesos que recibirán dichos reportes.
- Consistente: Los reportes deben ser consistentes a lo largo del tiempo, para que la información sea comparable entre reportes y permita la detección de desviaciones y tendencias a lo largo del tiempo.
- Interpretable: La información reportada debe ser entendible por la audiencia objetivo.

4.2.6.3. Proceso de establecimiento de KRIs.

4.2.6.3.1. Evaluación del riesgo.

Como prerrequisito previo para la definición y evaluación de KRIs, debe identificarse los riesgos más relevantes que impacten en los ecosistemas tecnológicos de la organización, incluyendo los servicios cloud adquiridos.

Los riesgos que a identificar y evaluar deben comprender todas las dimensiones con impacto tecnológico, y no exclusivamente aquellos asociados a la ciberseguridad, incluyendo también aspectos de continuidad, gestión de proveedores, calidad del dato, y aspectos operacionales y de cumplimiento.

4.2.6.3.2. Definición de KRIs.

Con los principales riesgos identificados, el siguiente paso es definir una estructura de métricas que cubra dichos riesgos, priorizando y ofreciendo una cobertura reforzada a aquellos riesgos con mayor impacto o probabilidad de materialización sobre la organización.

Al igual que ocurre con los KPIs, los KRIs deben definirse garantizando que sean representativos, específicos, medibles, alcanzables, realistas y acotados en el tiempo. Asimismo, en el caso de los KRIs debe lograrse una combinación de indicadores predictivos y de indicadores detectivos, de forma que sea posible analizar tanto los riesgos materializados, como aquellos que presenten indicios de materialización en el corto plazo.

Los KRIs que se definan deben considerar los distintos ecosistemas a evaluar. Aunque varios KRIs evalúen un mismo riesgo, éstos deberán considerar la arquitectura de despliegue del recurso analizado, para que ofrezcan un resultado homogéneo del riesgo y al mismo tiempo adaptado a cada elemento sobre el que dicho riesgo podría materializarse. En este sentido, los KRIs evaluados sobre recursos en la nube serán más dependientes de los reportes e información facilitada por el CSP, especialmente en aquellos modelos de servicio en los que el CSP gestione un gran número de capas de la infraestructura cloud.

4.2.6.3.3. Establecimiento de objetivos y límites.

Los KRIs deben contextualizarse para adaptarse a los requerimientos de la organización. Para ello, todo KRI que sea medido debe poseer un valor objetivo y un límite aceptable, de forma que cada medición pueda compararse con la situación ideal para ese KRI, y determinarse si los valores de riesgo se encuentran dentro de los límites aceptables de la organización.

Los valores objetivo definidos para cada KRI deben ser consistentes con la estrategia de gestión del riesgo de la organización, mientras que los límites aceptables deben respetar el apetito al riesgo aprobado.

4.2.6.3.4. Evaluación y monitorización.

La organización deberá definir la frecuencia con la que realizará mediciones de los KRIs definidos y los comparará con los valores objetivo y límites. Aunque se trata de un proceso iterativo, dependiendo de los niveles de riesgo previamente cuantificados, podrán existir KRIs que no se midan en todas las iteraciones, cuando los riesgos asociados sean de baja criticidad para la organización.

El proceso de evaluación de KRIs puede implantarse utilizando diversas técnicas, aunque puesto que uno de los objetivos de CA&CM es lograr una ejecución continua, será preferible optar por técnicas que logren altos niveles de automatización.

Si bien no todos los KRIs o riesgos tienen por qué ser evaluados en cada iteración, cuando se analice un determinado riesgo en una iteración, es recomendable que este se analice sobre todos los ecosistemas y recursos tecnológicos sobre los que éste aplique, para obtener una visión clara de la superficie de impacto de cada riesgo de forma global a la organización. La única excepción a estar regla son aquellos recursos tecnológicos de criticidad despreciable, que podrán omitirse en determinadas iteraciones para lograr mayor eficiencia.

4.2.6.3.5. Reporte.

Una vez medidos y analizados los KRIs, los resultados de este proceso deberán ser integrados en el proceso de CRMA, y reportados a los órganos de gobierno y control que corresponda, así como a las áreas involucradas en el tratamiento y control de los riesgos identificados.

A la hora de generar los reportes sobre KRIs, además de incorporar información sobre las mediciones y desviación frente a valores objetivo y límites de la iteración actual, también debe incorporarse información histórica y agregada que permitan identificar tendencias y desviaciones a lo largo del tiempo.

4.2.6.3.6. Retroalimentación.

Tras la realización del reporte, el proceso debe analizarse para garantizar que los KRIs, sistemas de evaluación, y valores objetivo y límite, siguen estando alineados con las necesidades y requerimientos de la organización.

De esta etapa podrá realizarse alguna modificación en estos valores, o determinarse la necesidad de incrementar o reducir el número de KRIs que soporten la evaluación de un determinado riesgo, para que el proceso de evaluación de KRIs ofrezca información relevante y de valor para la organización y se adapte a los cambios que se produzcan en la organización o en su contexto.

Aunque en el caso de la gestión del riesgo sobre un servicio cloud existe una elevada dependencia del CSP, y la introducción de cambios estará sujeta a las restricciones estipuladas en el contrato con el proveedor, es importante mantener el proceso actualizado también en estos entornos y tratar de mantener la supervisión de KRIs alineada con las necesidades de la organización.

4.2.6.4. Consideraciones a la hora de definir KRIs en cloud.

4.2.6.4.1. Relevancia.

Uno de los mayores retos a la hora de definir KRIs es lograr que éstos sean relevantes para cubrir el riesgo correspondiente y que sean representativos a partir del recurso sobre el que se evalúan.

Esto es incluso más complejo en el caso de servicios cloud, puesto que el acceso a información técnica detallada está más restringido. Por tanto, la evaluación de KRIs en su conjunto debe balancear la obtención de información desde fuentes técnicas, en el caso de aquellas capas de la infraestructura gestionadas por el cliente; y de reportes facilitados por el CSP y acordados contractualmente, para las capas o procesos gestionados por el CSP.

4.2.6.4.2. Selección de un catálogo completo.

La selección del catálogo de KRIs también es una labor compleja, especialmente cuando existe ecosistemas tecnológicos heterogéneos, como es el caso de organizaciones que hagan uso de servicios en la nube. Para ofrecer una visión global y consistente a lo largo de toda la organización, las métricas utilizadas por los KRIs deben evaluar los riesgos considerando los recursos sobre los que éstos pueden impactar, pero abstrayendo el resultado de la medición de las características técnicas de los recursos tecnológicos, para ofrecer una visión homogénea de los riesgos.

Asimismo, el número de KRIs para cubrir riesgos con una mayor criticidad para la organización deberá ser mayor que aquellos asociados a riesgos poco críticos. De la misma manera, cuando un riesgo resulte complejo de medir en un determinado ecosistema, éste deberá soportarse por un mayor número de KRIs, para que ofrezcan un nivel de detalle lo más similar posible a la evaluación de dicho riesgo sobre el resto de los ecosistemas.

4.2.6.4.3. Considerar todo el contexto del riesgo.

La gestión del riesgo en la organización es un proceso complejo. Por tanto, los KRIs no deben medir exclusivamente los riesgos, sino cualquier elemento que sea relevante para su identifica-

ción o tratamiento. Entre estos elementos, puesto que los servicios cloud son gestionados en cierta medida por el CSP, deberá incluirse la capacidad de gestión del riesgo del CSP, incorporar aquellos riesgos introducidos por el CSP, y tener en cuenta su interacción en la gestión del riesgo llevada a cabo por la organización.

4.2.6.4.4. Uso de información de calidad.

La capacidad de un KRI para aportar información de valor a la organización vendrá determinada en gran medida por la calidad de la información utilizada para la evaluación de dicho KRI. En el caso de aquella información que se obtenga directamente del entorno cloud, ésta deberá ser validada antes de su análisis. Para ello, una opción es utilizar analítica de datos para la medición de KRIs. En el caso de la información que deba facilitar el CSP, deberán acordarse con éste los requerimientos mínimos de calidad, y definirse mecanismos para poder evaluar dicha calidad.

4.2.6.4.5. KRIs sobre el CSP y el servicio medidos por el propio CSP.

Determinados KRIs serán difícilmente medibles por parte de la organización. Puesto que la mayoría de los contratos incluyen SLAs, puede resultar beneficioso incluir además la medición de métricas que cubran requerimientos no funcionales por parte del CSP. Entre estas mediciones pueden incluirse KRIs, si bien deberán definirse a nivel contractual, y exigir toda la información de soporte necesaria que permita evaluar la idoneidad de las mediciones realizadas por el CSP, para asegurar que la información provista es de calidad. Todas estas responsabilidades, independientemente de si el KRI se evalúa por la organización o por el CSP deben explicitarse contractualmente de forma precisa y detallada.

5 ESTRATEGIA DE EJECUCIÓN Y DESARROLLO

5.1. Modelo de ejecución.

Aunque generalmente se entiende por auditoría y monitorización continuas el uso de métodos para incrementar la periodicidad con la que se ejecutan las labores de auditoría y monitorización, llegando en un punto ideal a ejecutarlas de forma constante, este modelo de supervisión suele estar principalmente relacionado con el uso de herramientas que automaticen el proceso.

CA&CM comprende la ejecución de 3 procesos de supervisión (CDA, CCM y CRMA), y por tanto en el presente documento se ha optado por un enfoque de ejecución que se centre en cómo abordar dichos procesos, más que en herramientas puntuales que favorezcan su automatización. Otro motivo por el que se ha optado por un enfoque de ejecución centrado en procesos y no en herramientas es que dicho enfoque aporta una visión que favorece su integración con los procesos de asesoramiento y aseguramiento ejecutados como parte de la función de Auditoría Interna.

Una vez diseñados los procesos de CA&CM para su ejecución, la selección de herramientas que logren su automatización total o parcial resulta trivial, a partir de las necesidades y requerimientos tanto de la organización como de la función de Auditoría Interna.

5.1.1. Aspectos básicos del modelo de ejecución.

5.1.1.1. Modelo iterativo.

Uno de los elementos fundamentales que definen los procesos de CA&CM es que su ejecución debe ser periódica, y en el mejor de los casos continua. Por tanto, es imprescindible que el modelo de ejecución se base en ciclos de iteración, o modelo de mejora continua.

Este modelo iterativo podrá basarse en el ciclo de Deming (PDCA) o en el cualquier otro modelo iterativo, como el que propone la metodología ágil Scrum. El requerimiento fundamental del mo-

delo seleccionado es que permita la obtención de resultados con cada iteración, y que favorezca la mejora continua, mediante fases dedicadas al análisis y mejora del proceso a ejecutar.

Uno de los requerimientos fundamentales de la iteración en el modelo propuesto, como ocurre con Scrum, es que su duración debe ser fija, de forma que el tiempo transcurrido desde el inicio de la iteración hasta su finalización sea el mismo para todas ellas. Aunque es posible realizar ajustes si se considera que el tiempo de iteración se ha establecido de forma incorrecta, es conveniente que se realicen el mínimo número posible de ajustes.

5.1.1.2. Uso de principios ágiles.

Basar la ejecución de los procesos CA&CM en principios ágiles garantizará no solo el incremento en el aporte de valor y el alineamiento con las necesidades del negocio, sino una ejecución más fluida de éstos, lo que resulta imprescindible para lograr la ejecución continua requerida por CA&CM.
Los principios ágiles que habrá que aplicar, adaptados a la ejecución de auditorías basadas en CA&CM, son los siguientes:

- La función de aseguramiento debe buscar el soporte y tener una comunicación fluida con el CSP y con las áreas de la organización, de forma que no se centre exclusivamente en la identificación y tratamiento del riesgo sino en el entendimiento de éste desde la perspectiva de las partes interesadas.

- Cada ciclo de iteración debe ofrecer aseguramiento a la organización, y garantizar el tratamiento de los riesgos identificados, en lugar de invertir iteraciones en obtener un modelo de supervisión demasiado maduro pero que no aporte resultados.

- La relación con el CSP y con el resto de las partes interesadas debe gestionarse con una visión de aporte de valor mutuo, y no como un modelo de supervisión en el que la función de Auditoría Interna actúa de forma arbitraria sin tener en cuenta las necesidades de las partes interesadas.

- Es preferible centrarse en el contexto y necesidades de la organización y saber adaptarse a ellos, que seguir una planificación fijada que provoque el desalineamiento de la función de aseguramiento.

5.1.1.3. Enfoque incremental de madurez.

A medida que la función de aseguramiento se vaya desarrollando sobre el servicio cloud, y vaya integrándose con los procesos de CA&CM, deberán realizarse las adaptaciones necesarias para incrementar el aporte de valor de dichos procesos a la organización.

Es preferible empezar a integrar los procesos de CA&CM con la función de aseguramiento, aunque los resultados de dicha integración no sean inicialmente excesivamente fluida, antes que tratar de integrar dichos procesos una vez que estén suficientemente maduros como para que el aporte de valor a la función de aseguramiento sea significativo. De lo contrario, es probable que la integración nunca llegue a producirse.

5.1.1.4. Balanceo entre la automatización y la integración.

Aunque el objetivo último de CA&CM es que la supervisión se lleve a cabo de forma continua, considerando su integración con la función de aseguramiento, esto puede provocar ciertas dificultades, puesto que la supervisión de determinados riesgos y controles no serán fácilmente automatizables.

Será preferible una integración mayor entre CA&CM y la función de aseguramiento, aún a costa de una reducción en la frecuencia de supervisión, siempre que dicha frecuencia no sea inferior a la de evaluación mediante las técnicas de auditoría tradicionales, lo cual resulta improbable considerando que la mayoría de los recursos tecnológicos de una organización ni siquiera se auditan de forma anual.

Una vez que se haya logrado un nivel de integración satisfactorio, es conveniente tratar de incrementar la frecuencia con la que se producen las revisiones, pero sin que dicho incremento impacte en el alcance de las revisiones, puesto que éstas deben cubrir los recursos críticos para la organización y los principales riesgos con impacto en éstos. La única excepción que se plantea a esta afirmación se da durante las fases iniciales de madurez del modelo, en las que no siempre será posible cubrir todos los recursos y riesgos relevantes para la organización desde el inicio.

5.1.2. Por qué usar un modelo iterativo basado en principios ágiles.

El modelo de ejecución propuesto para los procesos que conforman CA&CM se basa en un modelo iterativo que hace uso de principios ágiles.

Los motivos por los que se ha optado por este tipo de modelo de ejecución, basados en las ventajas de los modelos iterativos y de las metodologías ágiles, se enumeran a continuación:

Este modelo iterativo podrá basarse en el ciclo de Deming (PDCA) o en el cualquier otro modelo iterativo, como el que propone la metodología ágil Scrum. El requerimiento fundamental del modelo seleccionado es que permita la obtención de resultados con cada iteración, y que favorezca la mejora continua, mediante fases dedicadas al análisis y mejora del proceso a ejecutar.

Uno de los requerimientos fundamentales de la iteración en el modelo propuesto, como ocurre con Scrum, es que su duración debe ser fija, de forma que el tiempo transcurrido desde el inicio de la iteración hasta su finalización sea el mismo para todas ellas. Aunque es posible realizar ajustes si se considera que el tiempo de iteración se ha establecido de forma incorrecta, es conveniente que se realicen el mínimo número posible de ajustes.

5.1.1.2. Uso de principios ágiles.

Basar la ejecución de los procesos CA&CM en principios ágiles garantizará no solo el incremento en el aporte de valor y el alineamiento con las necesidades del negocio, sino una ejecución más fluida de éstos, lo que resulta imprescindible para lograr la ejecución continua requerida por CA&CM.
Los principios ágiles que habrá que aplicar, adaptados a la ejecución de auditorías basadas en CA&CM, son los siguientes:

- La función de aseguramiento debe buscar el soporte y tener una comunicación fluida con el CSP y con las áreas de la organización, de forma que no se centre exclusivamente en la identificación y tratamiento del riesgo sino en el entendimiento de éste desde la perspectiva de las partes interesadas.

- Cada ciclo de iteración debe ofrecer aseguramiento a la organización, y garantizar el tratamiento de los riesgos identificados, en lugar de invertir iteraciones en obtener un modelo de supervisión demasiado maduro pero que no aporte resultados.

- La relación con el CSP y con el resto de las partes interesadas debe gestionarse con una visión de aporte de valor mutuo, y no como un modelo de supervisión en el que la función de Auditoría Interna actúa de forma arbitraria sin tener en cuenta las necesidades de las partes interesadas.

- Es preferible centrarse en el contexto y necesidades de la organización y saber adaptarse a ellos, que seguir una planificación fijada que provoque el desalineamiento de la función de aseguramiento.

5.1.2.1. Mayor adaptación al proceso.

Dado que CA&CM se fundamenta en la ejecución periódica (idealmente continua) de procesos de supervisión, el uso de un modelo iterativo de tipo PDCA ofrece un buen alineamiento con éstos, puesto que ambos poseen una estructura de ejecución similar.

5.1.2.2. Mejora la flexibilidad.

A medida que se ejecuten iteraciones de los procesos que forman CA&CM será necesario realizar ajustes, incluyendo el incremento de los elementos analizados o en la automatización en los procesos de recopilación de información y análisis. Un proceso iterativo favorece la introducción de cambios a medida que éstos se consideren necesarios.

Adicionalmente, puesto que los entornos cloud, que ofrecen tecnología como servicio, poseen un elevado nivel de flexibilidad y elasticidad, contar con un modelo de supervisión que también posea estas características ayudarán a obtener una supervisión más eficiente y a integrar el análisis de servicios cloud en la función de aseguramiento.

5.1.2.3. Ofrece resultados más rápido.

A diferencia de los modelos de implementación basados en fases secuenciales en lugar de en ciclos de iteración, los modelos iterativos permiten mostrar resultados antes de que haya finalizado de forma completa la ejecución. De esta manera, aunque no ofrecen resultados finales desde el inicio, sí que permiten ir mostrando los resultados parciales de cada iteración, lo que permite trasladar el aporte de valor de forma más rápida.

A la hora de analizar servicios en la nube, considerando la mayor incertidumbre que existe sobre éstos en lo que respecta al análisis y tratamiento de los riesgos, por ser entornos tecnológicos gestionados por un tercero, poder obtener resultados de forma frecuente garantizar un mejor aseguramiento a lo largo del tiempo.

Por otro lado, los procesos que forman CA&CM tienden hacia la ejecución continua, por lo que debe utilizarse un modelo de ejecución que ofrezcan resultados de forma frecuente.

5.1.2.4. Mejora la integración.

Puesto que los procesos CA&CM no están habitualmente integrados en la función de aseguramiento de las organizaciones, contar con un modelo de ejecución iterativo fundamentado en principios ágiles favorecerá una integración más progresiva, pudiendo corregir aquellos aspec-

tos que provoquen desalineamientos con la función de aseguramiento, y reduciendo el coste asociado a la ejecución de correcciones sobre el modelo de supervisión, por ser éstas de menor amplitud en la medida en la que se reduzca la carga de cada iteración.

5.1.2.5. Optimiza los recursos.

La ejecución de CA&CM haciendo uso de principios ágiles permite centrar cada iteración en los aspectos más relevantes en cada momento, y garantiza que los recursos se destinen a aquellas actividades y recursos que ofrezcan mayor aporte a la organización.

Teniendo en cuenta la incertidumbre existente a la hora de supervisar recursos externos, como son los servicios cloud, este modelo de ejecución también permitirá ir adaptando la supervisión a medida que se vaya obteniendo información de utilidad sobre los servicios cloud contratados y se vayan identificando los riesgos presentes en éstos.

5.1.2.6. Favorece el alineamiento con negocio.

La función de aseguramiento de las organizaciones debe adaptarse a su contexto, y cubrir los requerimientos de los órganos a los que ésta reporta, por lo que resulta beneficioso basar dicha función en un proceso de supervisión que se ejecuta frecuentemente, y no en ciclos anuales (en el mejor de los casos), como ocurre tradicionalmente con las auditorías basadas en modelos de aseguramiento estándar.

Habitualmente, el tiempo transcurrido desde que se identifica la necesidad de ofrecer aseguramiento sobre un proceso o recurso hasta que los riesgos asociados a éstos se identifican y evalúan es elevado. Con el uso de CA&CM y una ejecución de procesos iterativa se acelera la identificación de riesgos y su análisis, reduciendo los tiempos de espera hasta aportar resultados y conclusiones a los órganos de reporte, y acelerando el tratamiento de los riesgos identificados.

5.1.2.7. Mejora la participación de las partes interesadas.

Los principios de gestión ágiles ayudan a obtener la involucración de las partes interesadas, al incrementar la participación de éstas en los procesos que se ejecutan.

Sobre un servicio cloud, la introducción del CSP como una parte interesada más dentro del proceso de ejecución de auditorías favorecerá una comunicación fluida con éste, y ofrecerá un punto de vista más próximo entre ambas organizaciones, de forma que la función de auditoría interna no se perciba como un área aislada del resto de la organización, sino como una línea de control capaz de incrementar el aporte de valor y el alineamiento entre organizaciones.

5.1.2.8. Incremento constante de madurez.

Contar con una etapa en cada iteración del proceso de supervisión que identifique puntos de mejora y promueva la realización de las correcciones oportunas sobre el modelo de supervisión fuerzan a los procesos de CA&CM a su mejora continua.

Esto resulta ventajoso a la hora de supervisar cualquier recurso tecnológico o proceso, pero es especialmente útil en entornos cloud, puesto que las capacidades de supervisión están mucho más limitadas.

5.1.2.9. Favorece el control y la supervisión.

El análisis y evaluación periódica de los propios procesos de CA&CM como soporte a la función de Auditoría Interna de la organización ayuda a reducir el riesgo de control, dado que los procesos y las actividades de supervisión también son evaluados en busca de puntos de mejora.

Dado que la relación con el CSP y la infraestructura cloud durante la ejecución de auditorías puede resultar compleja, resultará de mucha utilidad poder identificar aspectos a tratar para que dicha relación sea lo más fluida y eficiente posible.

5.1.2.10. Aporta mayor transparencia.

Ejecutar los procesos de CA&CM utilizando principios ágiles ofrece más información a las partes interesadas. Aunque la ejecución de auditorías siempre debe estar fundamentada en una comunicación fluida y directa con dichas áreas, especialmente en lo relativo a la comunicación de riesgos identificados, este enfoque además ofrece mayor visibilidad sobre el proceso de auditoría.

5.1.3. Artefactos requeridos para la ejecución iterativa.

En capítulos anteriores se han identificado los elementos fundamentales que deben desplegarse para poder ejecutar CA&CM en una organización, especialmente cuando ésta haga uso de servicios cloud.

Adicionalmente, debe hacerse uso de elementos de soporte para la ejecución iterativa de estos procesos. Estos elementos no están orientados al aseguramiento y gestión del riesgo, sino que se usan para coordinar y soportar la ejecución de las iteraciones.

Estos elementos de soporte al modelo de ejecución, basados en los artefactos Scrum, son los siguientes:

5.1.3.1. Lista de Tareas Pendientes.

De forma similar a como ocurre con la lista de producto en Scrum, la lista de tareas contendrá un listado priorizado de aquellas tareas que se decida acometer como parte de los procesos CA&CM, siempre que éstas no comprendan la definición e implantación de elementos dependientes para los elementos clave, que se llevarán a cabo durante la fase de preparación, previa a la ejecución del primer ciclo.

El formato de la lista de tareas pendientes es el siguiente:

Tareas
Tarea #1
Tarea #2
Tarea #3

Tarea #N

Para cada tarea, se incluirá, además, una breve descripción que permita entender al equipo responsable de la implantación de CA&CM cuál es la finalidad de la tarea, qué requerimientos mínimos deben cumplirse para dar la tarea por completada, la prioridad asignada a dicha tarea, y una estimación de tiempo necesario para la ejecución de la tarea.

No es necesario que todas las tareas en la lista posean el mismo nivel de detalle. Será suficiente con que un número suficiente de ellas, que vendrá determinado por la capacidad del equipo para ejecutar tareas en una iteración, posea un nivel de detalle tal que permita su incorporación a la iteración actual. El resto, podrán irse definiendo durante la ejecución de las siguientes iteraciones.

El tamaño mínimo de la lista de tareas pendientes debería ser el suficiente para garantizar que hay tareas suficientes como para ejecutar una iteración de forma completa, aunque todas las tareas que se vayan identificando como necesarias para la ejecución de CA&CM deberán incorporarse.

La tipología de tareas incorporadas en lista de tareas pendientes, como se verá en secciones posteriores, irá cambiando a medida que el modelo de supervisión adquiera madurez. Si bien en las primeras iteraciones la mayoría de las tareas se basarán en la integración de nuevos elementos clave de supervisión en CA&CM, posteriormente éstas dejarán paso a otras destinadas a la medición periódica, depuración y optimización de estos elementos.

Un requisito fundamental de las tareas incorporadas en la lista es que éstas deben ser independientes entre sí.

Esta lista se actualizará constantemente, a medida que se vayan identificando tareas que resulte necesario ejecutar, y nunca podrá vaciarse completamente, puesto que eso supondría romper con el modelo de mejora continua. Sin embargo, sí podrá ocurrir que las tareas introducidas se vuelvan repetitivas, como, por ejemplo, para representar la necesidad de medir y analizar un conjunto particular de elementos clave de supervisión en cada una de las iteraciones.

La necesidad de ejecutar de forma constante estas tareas podrá representarse en la Lista de Tareas Pendientes de forma que dichos elementos, una vez seleccionados para la iteración actual, no se eliminen de la lista de tareas pendientes, sino que simplemente se reevalúe su prioridad dentro de ésta.

Por último, es importante tener en cuenta que existe la posibilidad de eliminar una tarea de la lista de tareas pendientes, cuando se considere, independientemente de si ya se ha incorporado en alguna iteración o si nunca se ha ejecutado, que no es necesaria.

5.1.3.2. Matriz de Integración.

La ejecución de CA&CM, tal y como ha sido planteada, requiere del análisis de tipologías o conceptos de datos, controles, KPIs y KRIs.

En última instancia, el objetivo de CA&CM es que se produzca un análisis continuo de todos estos elementos. Para poder llegar a dicho objetivo todos ellos deben definirse, implantarse, analizarse y depurarse.

En el modelo de ejecución planteado, estos elementos no necesariamente se integran de forma completa desde el inicio, de tal forma que, por ejemplo, para finalizar la primera iteración, no será necesario que la organización cuente con un conjunto completo de KPIs y KRIs que analice todos los controles y riesgos respectivamente.

En su lugar, tras la ejecución de las sucesivas iteraciones, el número de elementos a analizar se irá incrementando.

Para controlar los elementos que se irán introduciendo en el proceso de CA&CM en cada iteración, se usará la matriz de integración, que contendrá una priorización de los elementos clave de supervisión en CA&CM.

Esta estructura no se corresponde con ningún elemento definido en Scrum, si bien será una estructura intermedia entre la lista de producto (aquí llamada lista de tareas) y la lista de pendientes del sprint (referenciada como lista de iteración).

La matriz, que se representa gráficamente a continuación, contendrá una priorización de todos los elementos a supervisar.

Datos	Actividades	Controles	KPIs	KRIs
Dato #1 (C)	Actividad #1 (C)	Control #1 (C)	KPI #1 (C)	KRI #1 (C)
Dato #2 (C)	Actividad #2 (C)	Control #2 (C)	KPI #2 (C)	KRI #2 (C)
Dato #3 (C)	Actividad #3 (C)	Control #3 (C)	KPI #3 (C)	KRI #3 (C)
Dato #N (C)	Actividad #N (C)	Control #N (C)	KPI #N (C)	KRI #N (C)

(C): {"(I)" Integrar | "(A)" Analizar | "(D)" Depurar}

El código que se incorpore entre paréntesis a continuación del elemento clave de supervisión incluido en la matriz permitirá identificar la acción que desea llevarse a cabo sobre dicho elemento, con la única restricción de que no pueden analizarse o depurarse elementos que no se hayan integrado previamente, aunque sí podrá analizarse un elemento que se haya integrado en esa misma iteración.

De la misma manera que la lista de tareas, esta matriz no tiene por qué contener una lista exhaustiva de todos los elementos que se implantarán durante la ejecución de CA&CM, sino únicamente aquellos que ya se hayan considerado para su integración o sobre los que se desee iterar. Siempre que en la lista de tareas pendientes se incluya la interacción con algún elemento clave de supervisión, dicho elemento deberá obtenerse de los elementos superiores en la matriz de la integración, de forma que la tarea se traslade a la lista de iteración junto con los elementos de mayor prioridad en la matriz de integración que contengan el mismo tipo de acción que la incluida en la lista de tareas pendientes.

En caso de que se finalice la iteración y no se haya ejecutado alguna acción sobre los elementos seleccionados, éste será devuelto a la matriz en el orden que se considere oportuno.

Esta matriz nunca podrá vaciarse, puesto que no iterar sobre los elementos clave de supervisión supondrá no producir aporte de valor, y toda la ejecución de los procesos de CA&CM se basa en la interacción con elementos clave de supervisión. Sin embargo, a medida que CA&CM vaya adquiriendo madurez, dejarán de figurar elementos para su integración, y la actividad se centrará en su análisis y depuración.

5.1.3.3. Lista de Iteración.

Una vez que un elemento de la lista de tareas pendientes se ha incorporado en la iteración actual, las tareas seleccionadas deben detallarse y descomponerse en subtareas, hasta obtener un nivel de granularidad suficiente como para que los miembros del equipo encargados de la ejecución de CA&CM puedan ejecutar las subtareas de forma autónoma, sin requerir excesiva supervisión.

También es importante que las subtareas sean lo suficientemente granulares como para que la evolución en su ejecución sea visible de forma rápida (idealmente diariamente). De esta manera, una subtarea, como mucho, debería poderse completar en un día.

En este caso, la Lista de Iteración consiste en una estimación de todas las tareas que podrán ejecutarse durante la Iteración, a partir de la dedicación estimada para cada tarea, y el ritmo promedio de ejecución de las iteraciones previas.

A continuación, se presenta un ejemplo de lista de iteración:

Tareas				
Tarea #1	Subtarea #1.1	Subtarea #1.2	Subtarea #1.3	
Tarea #2	Subtarea #2.1	Subtarea #2.2		
Tarea #3	Subtarea #3.1	Subtarea #3.2	Subtarea #3.3	Subtarea #3.4
Tarea #i	Subtarea #i.1	Subtarea #i.2		Subtarea #i.j

Los elementos incorporados en esta lista no pueden modificarse una vez iniciada la fase de ejecución de la iteración. Cuando se identifique la necesidad de ejecutar una nueva tarea, ésta deberá incorporarse a la lista de tareas pendientes, y las tareas ya ejecutadas se marcarán para reflejar que no deben devolverse a la lista de tareas pendientes tras la finalización de la iteración.

Las tareas que requieran interacción con elementos clave de supervisión, cuando se incorporen a la lista de iteración, deberán asociarse de forma explícita a uno o más elementos clave de supervisión. Esta agrupación la decidirá el responsable del aseguramiento o el mánager de auditoría, de forma que el agrupamiento seleccionado para una tarea cubra un objetivo común o complementario.

5.1.3.4. Aporte al aseguramiento.

El Aporte al aseguramiento, de manera similar a los Incrementos en Scrum, representa el resultado de la ejecución de todas las iteraciones ya finalizadas.

A diferencia de los Incrementos en Scrum, el aporte al aseguramiento, aunque la iteración se haya completado satisfactoriamente, no necesariamente supone una versión mejorada del producto, en este caso el aseguramiento frente al riesgo; sino que simplemente puede reflejar una actualización de dicho aseguramiento, de forma que ofrezca información idéntica a la obtenida previamente, pero actualizada en el tiempo.

5.1.4. Roles involucrados en la implantación y ejecución de CA&CM.

Existen diversos perfiles involucrados en la función de aseguramiento de una organización. Para la ejecución de CA&CM, al menos, deben considerarse los siguientes:

5.1.4.1. Responsable del aseguramiento.

El responsable del aseguramiento, que en este caso estaría representado por la figura del Director de Auditoría de TI, es el encargado de determinar la estrategia de aseguramiento.

Su función a la hora de implantar y ejecutar CA&CM es priorizar aquellas tareas que deben ejecutarse y elementos clave que deben ser tenidos en cuenta en las iteraciones.

Debe servir de punto de unión con las partes interesadas, asegurarse de que las necesidades de aseguramiento de la organización están convenientemente cubiertas, y comunicarse con éstas para aportar transparencia al proceso de CA&CM y obtener feedback de su ejecución.

5.1.4.2. Equipo de auditoría.

El equipo de auditoría, a cargo de la ejecución del trabajo de campo como parte de las auditorías, será el encargado de ejecutar los procesos de CA&CM y de realizar las tareas necesarias para su ejecución y el aporte de aseguramiento a la organización.

Aunque cada miembro del equipo tendrá un determinado nivel de especialización en determinadas tareas o tipos de auditoría, todos los miembros deben ser capaces de ejecutar las tareas de integración y ejecución de CA&CM.

A diferencia de Scrum, estos equipos no trabajan de forma independiente, sino que deben reportar al Mánager o Supervisor del equipo, puesto que éste es el responsable de velar por el alineamiento entre el trabajo realizado y las expectativas del responsable del aseguramiento. Esto se debe a que, aunque Scrum trata de eliminar la figura del Project Mánager, en auditoría interna es recomendable que haya una diferenciación entre el equipo que ejecuta los trabajos y el responsable de su supervisión, para que el trabajo cuente con la profundidad necesaria sin perder la perspectiva de los objetivos y alcance de la actuación, haciendo que esta figura resulte necesaria.

5.1.4.3. Mánager / Supervisor del equipo.

Este rol se encarga tanto de la supervisión del trabajo de auditoría, como de garantizar que los principios del modelo de CA&CM se mantienen, ofreciendo asesoramiento al responsable del aseguramiento y al equipo de auditoría.

Por un lado, aportará información técnica al responsable del aseguramiento para que éste pueda definir las tareas de forma suficientemente detallada, y le ayudará a adaptar la estrategia de supervisión a CA&CM, así como a elaborar los reportes que se distribuirán entre las partes interesadas.

Por otro lado, supervisará al equipo de auditoría en la ejecución de funciones de aseguramiento y en la implantación y ejecución de CA&CM, resolviendo cualquier dificultad que éstos encuentren durante la ejecución del trabajo, tanto desde un punto de vista técnico, como organizativo y funcional, especialmente relevante a la hora de asegurar una comunicación fluida con el CSP y las áreas auditadas.

5.1.4.4. Partes interesadas.

Las partes interesadas serán las receptoras del aporte de valor generado por los procesos de CA&CM, así como aquellas involucradas en la ejecución de dichos procesos.

Hay tres partes interesadas fundamentales en un modelo CA&CM que supervise servicios cloud:

5.1.4.4.1. Comité de Auditoría / Consejo de Administración.

Es el órgano al que reporta Auditoría Interna, por lo que, a partir de sus inquietudes y preocupaciones, se diseñarán y mantendrán los elementos clave de CA&CM y se elaborarán los reportes sobre la situación y tratamiento de los riesgos identificados.

5.1.4.4.2. CSP.

Participará en diversos puntos en el proceso de auditoría, desde el aporte de información para alimentar los procesos de CA&CM, como para ejecutar las correcciones necesarias para el tratamiento de los riesgos identificados. En cualquier caso, su participación deberá estar regulada a nivel contractual.

5.1.4.4.3. Áreas auditadas internas.

En general, cualquier área de la organización podrá verse involucrada en la ejecución de auditorías, ya sea para la provisión de información sobre un determinado proceso, recurso o control; como para el establecimiento de medidas correctoras que traten los riesgos identificados.

Para la implementación de CA&CM también podrá requerirse la participación de áreas puntuales para lograr que la adquisición de determinada información o su análisis se lleven a cabo de forma automatizada.

5.1.5. Fases de la ejecución.

5.1.5.1. Preparación.

Esta primera fase del modelo se ejecutará una única vez, y comprenderá la ejecución de todas aquellas actividades que sean necesarias para poder iniciar la primera iteración de CA&CM.

Para ello, deberán identificarse todos los elementos de los que se consideran dependientes los elementos clave. Dependiendo del nivel de madurez de la organización, será necesario definir e implantar aquellos que aún no se hayan implementado.

Además, durante esta fase también se crearán todas las estructuras de soporte necesarias para poder ejecutar CA&CM.

5.1.5.1.1. Subfases.

5.1.5.1.1.1. Asignación de Responsabilidades.

Lo primero que es necesario realizar como parte de esta fase es la definición del equipo involucrado en la ejecución de CA&CM. A diferencia de la aplicación de metodologías ágiles sobre otros procesos, en los que hay más flexibilidad a la hora de seleccionar los miembros del equipo, en este caso, los roles se asignarán a los mismos perfiles en la mayoría de los casos.

Como se ha indicado anteriormente, el rol de responsable del aseguramiento la asumirá el Directorio de Auditoría Interna de TI, el equipo de auditoría estará formado exclusivamente por auditores, y el Mánager / Supervisor del equipo se asignará al auditor más cualificado para supervisar al equipo y dar soporte al responsable del aseguramiento.

5.1.5.1.1.2. Identificación exhaustiva de partes interesadas.

La ejecución de procesos bajo principios ágiles requiere una mayor comunicación con la organización y actores externos.

Aunque ya se han identificado como partes interesadas al Comité de Auditoría, al CSP, y al resto de áreas auditadas, deberá procederse a una identificación exhaustiva de éstas, analizando las diferencias entre ellas con un nivel de granularidad elevado, para que el reporte de resultados se haga lo más adaptado posible.

5.1.5.1.1.3. Identificación de expectativas de las partes interesadas.

Con las partes interesadas identificadas, deben agendarse reuniones con éstas para recabar su feedback sobre las expectativas del proceso.

Será responsabilidad del equipo encargado del aseguramiento interpretar la información aportada, y diferenciar aquellos aspectos que pueden ofrecer aporte de valor al proyecto, de aquellos que estén motivadas más por preocupaciones puntuales, que por una necesidad real de aseguramiento.

Un actor clave a consultar en este punto es el CSP, para que el equipo identifique el tipo de relación que podrá mantenerse con éste, así como la información que estará dispuesto a aportar, y la colaboración que cabe esperar durante el proceso.

Esta subfase ayudará no solo a identificar aspectos clave de los procesos de CA&CM, sino que también puede ser de utilidad para la selección de elementos clave a implantar. Sin embargo, es importante no perder la independencia de la función en este proceso.

5.1.5.1.1.4. Definición de los objetivos globales del proyecto.

Con toda la información recopilada de las partes interesadas, y con el conocimiento adquirido por el equipo de auditoría a lo largo del tiempo auditando la organización, deben establecerse objetivos globales del proyecto de integración de CA&CM en la función de aseguramiento de la organización.

En este punto será fundamental la involucración del responsable del aseguramiento, para favorecer que los objetivos y requerimientos planteados por las partes interesadas sean correctamente trasladados a objetivos de la función de aseguramiento y de los procesos de CA&CM.

En esta subfase aún no se definirán objetivos detallados, sino que esto se realizará durante la obtención de la Lista de Iteración. Sin embargo, es igualmente importante, puesto que todos los objetivos que se identifiquen sobre la Lista de Iteración deberán estar alineados con uno o más de los objetivos definidos en esta subfase.

5.1.5.1.1.5. Selección del conjunto mínimo viable de elementos clave.

Aunque la lista de elementos clave gestionada mediante CA&CM se irá incrementado a medida que se produzcan iteraciones, existe un número mínimo de ellos para que CA&CM aporte valor a la función de aseguramiento y a la organización.

Esta lista de número mínimo viable de elementos distinguirá no solo la tipología y características de un elemento, sino el recurso sobre el que éste interacciona.

Disponer de un análisis de riesgos formalizado y detallado será de gran utilidad para identificar cuáles son los elementos clave y recursos más relevantes, a partir de los riesgos con mayor impacto para la organización y los controles desplegados para su tratamiento.

5.1.5.1.1.6. Priorización inicial de elementos clave.

Los elementos clave incorporados en la Matriz de Integración deben priorizarse y ordenarse entre sí, para garantizar que no se quede sin implementar o evaluar un elemento que resulte más crítico para la organización que otro que sí se haya implementado o evaluado.

Con esta priorización, lo que se consigue es favorecer el máximo aporte de valor para la función de aseguramiento y para la organización con cada iteración.

Esta labor de priorización la deberá realizar el responsable del aseguramiento con el soporte del mánager del equipo.

5.1.5.1.1.7. Definición de los requerimientos generales de entrega.

Cada vez que se complete una tarea, o tras finalizar una iteración, deben existir unos requerimientos detallados y objetivos que permitan concluir sobre si la tarea o la iteración se han completado satisfactoriamente.

Aunque, en el caso de las tareas, cada una tendrá requerimientos específicos de finalización, también pueden existir requerimientos básicos que apliquen a todas ellas para garantizar un modelo suficientemente maduro y alineado con los requerimientos mínimos de la función de aseguramiento, que deberán ser definidos en esta subfase.

De la misma manera, también deberán establecerse formalmente que requerimientos debe cumplir el aporte de aseguramiento generado para resultar satisfactorio. Estos requerimientos pueden incluir distintos aspectos, como los formatos de reporte utilizados, los sistemas de análisis de elementos clave, etc.

Por último, también debe determinarse la duración de las iteraciones. Aunque generalmente para metodologías ágiles se recomienda que éstas no sean inferiores a una semana ni superiores a 4, dado que en este caso se está aplicando sobre la función de aseguramiento, debe escogerse un ciclo que sea lo suficientemente corto como para que el proceso pueda considerarse continuo, pero no lo suficientemente reducido como para que no se aprecie aporte de aseguramiento entre iteraciones.

5.1.5.1.2. Consideraciones.

Las consideraciones básicas a la hora de abordar esta fase son las siguientes:

- Aunque, a diferencia del resto, esta fase no tiene un límite de tiempo fijado, es recomendable no extenderla más de lo necesario, de forma que pueda empezarse a iterar lo antes posible.

- En caso de que el nivel de madurez de la organización en lo que respecta al aseguramiento sea bajo, o el set inicial de elementos a implantar sea elevado, puede ser recomendable realizar una iteración 0, en la que no se ofrezca feedback externo para asegurar que el equipo entiende sus funciones y determinar si las decisiones tomadas durante esta fase son acertadas.

5.1.5.2. Planificación.

En esta fase se diseñan y desarrollan todos los elementos que se verán involucrados en la fase de ejecución, para garantizar que éstos cuentan con un nivel de detalle suficiente y que todo el equipo es consciente del trabajo que debe desarrollar.

5.1.5.2.1.1. Análisis del contexto.

Al inicio de cada iteración, el equipo debe adquirir una visión actualizada del contexto de la organización, para poder identificar aquellos aspectos que son críticos para la organización, tanto a partir de la situación actual, como de la proyección de próximos pasos a ejecutar como parte de la estrategia de negocio.

Aunque esta subfase será más liviana que una evaluación inicial tradicional en el contexto del trabajo de auditoría, debe adquirirse un entendimiento mínimo para poder desarrollar las subfases que forman las fase de planificación, puesto que así se favorece el alineamiento continuo entre la organización y la función de aseguramiento.

5.1.5.2.1.2. Exposición y aclaración de los elementos de la Lista de Tareas Pendientes y de la Matriz de Integración.

A continuación, debe asegurarse que el equipo de auditoría comprende las tareas que es necesario ejecutar en la iteración en curso.

El responsable del aseguramiento, soportado total o parcialmente por el mánager de auditoría, debe trasladar sus expectativas para la iteración, mediante el desarrollo de los elementos de la

lista de tareas pendientes hasta que estos adquieran un nivel de detalle suficiente como para que sean incorporados en la lista de iteración.

Este mismo proceso también deberá realizarse sobre la matriz de integración, hasta determinar de forma precisa cómo deben integrarse o gestionarse los elementos clave incorporados a la iteración actual, para que produzcan los resultados de aseguramiento esperados.

Se trata de un proceso que no debe concluir hasta que todo el equipo posea una visión común sobre el contenido y objetivos de la iteración en curso.

5.1.5.2.1.3. Diseño de tareas a ejecutar.

Una vez entendidas las tareas incorporadas a la lista de tareas y los elementos clave en la matriz de integración, el equipo de auditoría debe desarrollar la Lista de Iteración, descomponiendo las tareas en subtareas, y dando suficiente nivel de detalle a los elementos clave.

Esta labor debe ser supervisada por el mánager de auditoría, para asegurar que se respetan los objetivos de la iteración y que se mantiene el enfoque trasladado por el responsable del aseguramiento.

Puede considerarse que esta subfase corresponde a la fase de diseño del programa de trabajo en una auditoría convencional, dado que el nivel de detalle que es necesario alcanzar es similar. Sin embargo, a diferencia de un programa de trabajo, en esta subfase aún no se han incorporado las tareas detalladas al proceso de aseguramiento mediante CA&CM.

El diseño de las tareas a ejecutar no se llevará a cabo sobre toda la lista de tareas pendientes, sino sobre el subconjunto que por la prioridad fijada entre el responsable del aseguramiento y el mánager de auditoría se consideren viables para su incorporación a la iteración en curso.

5.1.5.2.1.4. Selección de tareas y elementos clave de la iteración.

Cuando las tareas y elementos clave considerados para su integración o ejecución en los procesos de CA&CM poseen el nivel de detalle suficiente como para que el equipo de auditoría entienda qué resultados se esperan de su ejecución, éstas serán seleccionadas para su incorporación en la iteración.

El equipo de auditoría no seleccionará estos elementos de forma independiente, como ocurre en Scrum, sino que deberá ser una decisión consensuada entre todos los roles involucrados en CA&CM.

Esto es así a causa del impacto en la función de aseguramiento del momento en el que se aporten los resultados. Por ello, la gestión de elementos clave de supervisión mediante CA&CM debe considerar en qué momento se estima finalizar la próxima iteración, para que las conclusiones resulten relevantes en el momento en el que se exponen a las partes interesadas.

El motivo por el que esta tarea se lleva a cabo después del diseño de los elementos y no al revés, es que, dado que la iteración tiene un tiempo fijo, se necesita obtener un nivel de detalle mínimo

- ***5.1.5.2.1.5. Priorización de las tareas dentro de la iteración.***

Aunque las tareas ya se encuentran priorizadas en la lista de tareas pendientes, una vez desarrolladas e incorporadas a la iteración, se determinará en qué orden deben ejecutarse, considerando que aquellas posicionadas en último lugar corren el riesgo de no ejecutarse en la iteración actual y volver al listado de tareas pendientes. También deberá considerarse que una tarea de integración sobre un determinado elemento clave de supervisión deberá ejecutarse antes que otra de análisis o depuración sobre dicho elemento.

- ***5.1.5.2.1.6. Desarrollo de la Lista de Iteración (descomposición en subtareas).***

Llegados a esta subfase, se posee una lista de tareas priorizadas que poseen un nivel de detalle elevado, así como una matriz de integración igualmente detallada.

A continuación, deben descomponerse las tareas en subtareas, de tal forma que se llegue a un nivel de granularidad aceptable, y se permita hacer seguimiento diario del progreso de la iteración mediante el análisis de las subtareas completadas a lo largo del día previo.

Llegar a este nivel de detalle también favorece el entendimiento del equipo de auditoría, asegurando que no se produzcan desviaciones entre el resultado esperado y el resultado real tras la ejecución.

- ***5.1.5.2.1.7. Desarrollo de la Matriz de Integración.***

Tal y como se ha hecho en la subfase previa con el listado de tareas pendientes para obtener el listado de iteración, también debe incrementarse el nivel de detalle de los elementos clave, desarrollando todos los aspectos necesarios para su integración o gestión en la iteración actual. En este caso, un elemento clave que ya se encuentre integrado y sobre el que se quiera iterar requerirá un nivel de detalle menor, puesto que ya estará integrado, y su análisis deberá seguir las pautas definidas durante dicha integración.

5.1.5.2.2. Consideraciones.

Las consideraciones básicas a la hora de abordar esta fase son las siguientes:

- El tiempo que debe dedicarse a esta fase es variable, y se comparte con el tiempo de ejecución. De esta manera, en iteraciones poco maduras del proceso, en las que el número de elementos clave a gestionar sea reducido y los esfuerzos se centren más en la integración de nuevos elementos, esta fase requerirá una inversión mayor de tiempo, que posteriormente se irá cediendo a la fase de ejecución para la gestión de elementos clave.

- Como mínimo, esta fase ocupará un 5% del tiempo de la iteración, y como máximo un 40%.

- Todas las actividades dentro de esta fase requieren la supervisión estrecha del mánager de auditoría, puesto que el riesgo de perder el alineamiento con los objetivos de la iteración a medida que se van desarrollando los elementos es alto en este momento de la iteración.

- También será necesaria la participación del responsable del aseguramiento, aunque en menor medida que en el caso del mánager, especialmente para aportar un primer nivel de detalle sobre las tareas.

- Cuando un elemento de la lista de tareas pendientes se considere que debe ser corregido, por no estar bien definido, deberá ser descartado de la iteración actual, refinado, y devuelvo a la lista de tareas pendientes para su incorporación en una iteración posterior.

- Aunque el traspaso de elementos de la lista de tareas pendientes a la lista de iteración se lleva a cabo de forma consensuada entre todos los miembros, el responsable del aseguramiento en primer lugar, y el mánager de auditoría en segundo lugar, podrán imponer su criterio, aunque éste deberá justificarse para que el equipo de auditoría lo entienda.

5.1.5.3. Ejecución.

Durante esta fase se lleva a cabo el trabajo necesario para generar el aporte al aseguramiento, así como para desarrollar los procesos de CA&CM.

5.1.5.3.1. Subfases.

5.1.5.3.1.1. Mantener reuniones de seguimiento.

Los miembros del equipo de auditoría deben reunirse diariamente, siendo opcional la presencia del responsable del aseguramiento, para analizar la evolución de la iteración.

En cada reunión los miembros del equipo de auditoría deberán indicar qué tareas han ejecutado desde la reunión previa, qué tareas van a ejecutar a continuación, y los aspectos bloqueantes que se han encontrado.

El mánager de auditoría será responsable de aplicar las herramientas oportunas para analizar la evolución de los trabajos y de coordinar las correcciones o mejoras oportunas para garantizar el cumplimiento de los objetivos de la iteración. Adicionalmente, deberá identificar puntos de bloqueo que deberá resolver a nivel interno o con las partes interesadas, para que los trabajos de auditoría y los procesos de CA&CM se puedan ejecutar con normalidad.

5.1.5.3.1.2. Selección de tareas a ejecutar de la Lista de Iteración.

Aunque la ejecución de tareas de una iteración se acuerda al inicio de ésta, no se produce una asignación directa de tareas a cada miembro del equipo de auditoría. En su lugar, éstos van seleccionando tareas a medida que van acabando las que tenían previamente asignadas.

Puesto que las tareas se han dividido en subtareas, cada una de dichas subtareas se puede ejecutar de forma independiente. Sin embargo, como éstas pueden ser dependientes entre sí, el equipo deberá coordinarse para no ejecutar una subtarea dependiente de otra aún no finalizada, y para desarrollar la iteración del a forma más eficiente posible.

Un miembro del equipo de auditoría puede seleccionar más de una subtarea, si estima que puede completarlas en menos de un día y que existe una dependencia entre ellas por las que es necesario que la misma persona ejecute ambas.

5.1.5.3.1.3. Desarrollo de la subtarea seleccionada.

Una vez seleccionada una subtarea o un conjunto de ellas, el miembro del equipo de auditoría que se la ha asignado la ejecutará, sin que para ello existan restricciones en lo que respecta a las partes interesadas con las que deba interactuar, o los elementos que deba desarrollar o gestionar para completarla.

Aunque el desarrollo de las subtareas se realiza de forma autónoma, un miembro del equipo de auditoría puede requerir la colaboración puntual del mánager de auditoría, si por su complejidad o por requerir de toma de decisiones es necesario que éste intervenga.

- ***5.1.5.3.1.4. Dar soporte al resto de miembros (opcional).***

Una vez que un miembro del equipo de auditoría haya finalizado una subtarea, y antes de que se asigne la siguiente, es recomendable que éste ofrezca soporte al resto de miembros, dado que es posible que se haya producido algún bloqueo que pueda ayudar a resolver, y esto ayudará a incrementar la productividad general del equipo.

- ***5.1.5.3.1.5. Validar internamente subtareas ejecutadas y elementos clave sobre los que se ha iterado.***

Cuando una subtarea se haya ejecutado o un elemento clave ya haya sido integrado o gestionado en la iteración actual, éste deberá validarse frente a los requerimientos de finalización y objetivos.

Es el mánager de auditoría quien confirma si se ha finalizado una subtarea, aunque deben existir unos requerimientos formalmente establecidos sobre los que se realice dicha validación. Si un elemento no se ha finalizado correctamente, éste deberá corregirse, si la corrección es sencilla y puede llevarse a cabo en un tiempo despreciable; o ser devuelto a la lista de tareas pendientes si el tiempo de la iteración ya se ha agotado.

- ***5.1.5.3.1.6. Desarrollar la Lista de Tareas Pendientes.***

En cualquier momento de la fase de ejecución, el responsable del aseguramiento, o en su nombre el mánager de auditoría, pueden interaccionar con la lista de tareas pendientes y con la matriz de integración para añadir o desarrollar los elementos que se consideren oportunos.

Esta labor podrá realizarse teniendo en comunicación con las partes interesadas, dependiendo del estadio de madurez en el que se encuentren los procesos de CA&CM.

5.1.5.3.2. Consideraciones.

Las consideraciones básicas a la hora de abordar esta fase son las siguientes:

- El tiempo que debe dedicarse a esta fase depende del tiempo asignado a la fase de planificación. En conjunto, ambas actividades no deben superar el 75 % del tiempo de la iteración. Por tanto, si la fase de planificación ocupa un 5% del tiempo, la ejecución comprenderá un 75%; y si la planificación consume un 40%, la ejecución consumirá otro 40%.

- Aunque aquellas subfases a cargo del equipo de auditoría se llevarán a cabo de forma secuencial, las subtareas en las que participe el mánager de auditoría o el responsable del aseguramiento podrán llevarse a cabo en cualquier momento de la fase, con o sin la participación del resto de miembros del equipo.

- Existe mayor flexibilidad a la hora de validar una subtarea ejecutada en comparación con metodologías ágiles como Scrum, y en este caso se acepta la ejecución de correcciones si se estima que el tiempo requerido es poco y el aporte de éstas supera el aporte ofrecido por la selección de la siguiente subtarea.

- En esta fase, el responsable del aseguramiento trabaja de forma independiente al resto del equipo, y en general no se requiere su involucración para el desarrollo de las subfases a cargo del equipo de auditoría, que contarán con el soporte del mánager de auditoría.

- Cualquier elemento de la lista de iteración que no se haya completado al acabar el tiempo asignado a esta fase, será devuelto a la lista de tareas pendientes o a la matriz de integración, detallando qué falta para poder darlo por completado.

5.1.5.4. Revisión.

Esta fase se encarga de la presentación de resultados y reporte a las partes interesadas, a partir del aporte al aseguramiento conseguido. En este caso el reporte no se realizará necesariamente considerando exclusivamente el aporte al aseguramiento de la última iteración, sino que se deberá considerar el aporte completo y ofrecer una visión lo más actualizada posible sobre los aspectos incorporados en cada reporte.

5.1.5.4.1. Subfases.

5.1.5.4.1.1. Análisis de la evolución de los indicadores y controles.

Dado que una de las ventajas del modelo de CA&CM es que permite el análisis continuo de elementos clave, para incrementar el aporte de valor a la función de aseguramiento, el resultado de la ejecución de las iteraciones debe ser comparado, con el fin de obtener información sobre la evolución a lo largo del tiempo de los indicadores y controles, y aportar información que no solo represente una situación puntual, sino la evolución del riesgo a lo largo del tiempo.

5.1.5.4.1.2. Contraste de los resultados obtenidos con las partes interesadas.

Aunque los procesos de CA&CM son de ejecución continua y parcial o totalmente automatizados, los resultados obtenidos deben ser contextualizados, para validar que éstos aportan valor a la organización.

Para ello, los resultados obtenidos se compartirán con las áreas auditadas, incluyendo al CSP cuando se audite el servicio o la infraestructura cloud, y se recabará feedback de éstas. Sin que implique una pérdida de independencia, este contraste permitirá identificar fallos en el análisis realizado u obtener evidencias adicionales de relevancia que no hayan sido consideradas, e incluso contextualizar mejor los hallazgos obtenidos.

Es fundamental, para asegurar la independencia del proceso, que todas las correcciones, matizaciones y contextualizaciones realizadas por las partes interesadas durante este proceso estén soportadas por evidencias robustas, y que se corrijan los procesos de CA&CM o los elementos clave de supervisión para que las tengan en cuenta, cuando éstas se consideren relevantes y apropiadas.

5.1.5.4.1.3. Presentación de reportes de aseguramiento.

Una vez ejecutadas las subtareas y contrastados los resultados de su ejecución, se elaborarán los reportes resultantes de la integración y gestión de los elementos clave integrados en los procesos de CA&CM e incorporados a la iteración actual. Adicionalmente, para garantizar una visión completa del riesgo, deberá reportarse la situación y evolución del riesgo tecnológico y los elementos clave de supervisión a lo largo del tiempo, aunque un elemento particular no haya sido analizado en la iteración actual.

Hay que tener en cuenta que en esta subfase no se realiza un reporte directo del aporte al aseguramiento obtenido, sino que se adapta al público objetivo.

En esta subfase, se incluye el envío de conclusiones al CSP, para que las tenga en consideración de cara al mantenimiento y mejora del servicio. Debe darse soporte contractual a las acciones que el CSP deberá realizar con el reporte enviado, puesto que de no ser así no existen garantías de que éste sea de utilidad para la mejora del servicio.

5.1.5.4.1.4. Integración de reportes de aseguramiento en otros procesos de aseguramiento.

La información obtenida fruto de la ejecución de los procesos de CA&CM no se utilizará exclusivamente para su presentación a las partes interesadas.

Dependiendo de cómo se haya producido la integración de los procesos de CA&CM en la función de aseguramiento, será necesario incorporar dicha información a otros procesos de aseguramiento, como por ejemplo para la ejecución de auditorías, que tomarán como feedback la información aportada por CA&CM y realicen auditorías con un ámbito y alcance mucho más dirigidos.

Esta integración no se llevará a cabo de forma continua, ni siquiera en cada iteración, puesto que los ciclos de planificación y ejecución de la función de aseguramiento suelen ser extensos (habitualmente de un año). No obstante, dicha integración debe producirse, y puede aportar mucho valor a la función de auditoría interna, logrando un incremento sustancial en la optimización de los recursos y una cobertura mayor de los riesgos.

5.1.5.4.1.5. Presentación de avances y evolución en la ejecución de CA&CM.

Puntualmente, se deberá presentar a las partes interesadas clave, entre las que se incluye al menos al Comité de Auditoría o al Consejo de Administración, la evolución en la ejecución de los procesos de CA&CM, para que éstas puedan ver el resultado de su ejecución, y puedan aportar feedback no sobre éstos y sobre los resultados obtenidos.

5.1.5.4.1.6. Obtener feedback sobre los procesos y la iteración.

Una vez presentados los resultados a las partes interesadas, es conveniente obtener feedback periódico de éstas sobre los resultados de la iteración (el aporte al aseguramiento) y sobre los procesos de CA&CM.

A diferencia de los contrastes de resultados, la finalidad de esta sub-fase no es validar los resultados obtenidos, sino contrastar el aporte de valor para la organización del modelo de aseguramiento planteado.

5.1.5.4.2. Consideraciones.

Las consideraciones básicas a la hora de abordar esta fase son las siguientes:

- Esta fase será de duración fija dentro de la iteración, y ocupará el 10% del tiempo de ésta, para lo cual puede resultar necesario automatizar parte del proceso de generación de reportes.

- Una de las salvedades a la hora de aplicar principios ágiles sobre la función de aseguramiento con respecto a su uso para otras finalidades, es que aquí el reporte, aunque no debe ocupar un tiempo excesivo dentro de la iteración, podría llegar a producirse en cualquier momento, siempre que éste se considere oportuno y relevante.

- Debe analizarse el público objetivo de todos los reportes elevados y requerirse la involucración del responsable del aseguramiento en aquellos casos en los que éstos se dirijan a órganos de gobierno o control, como por ejemplo al Comité de Auditoría.

- Para aquellos reportes que se vayan a integrar en otros procesos de aseguramiento, la revisión por parte del responsable del aseguramiento no es imprescindible, pero al menos deberá llevarla a cabo el mánager de auditoría.

- El nivel de integración de los procesos de CA&CM con el resto de las actividades de la función de aseguramiento no debe ser completo, y es importante que se sigan ejecutando auditorías, dado que éstas permiten ofrecer un mejor nivel de aseguramiento. Las sinergias entre las auditorías tradicionales y CA&CM se produce cuando CA&CM permite la planificación y el diseño de auditorías con un alcance y objetivos más específicos gracias a toda la información aportada, y logra así una optimización de los recursos de CA&CM.

- En los reportes a las partes interesadas, deben diferenciarse muy bien los resultados obtenidos mediante CA&CM del resto de conclusiones emitidas por la función de auditoría interna, dejando claro que CA&CM ofrece resultados preliminares que deben ser contrastados de forma más exhaustiva.

- Aunque CA&CM no ofrezca un nivel de aseguramiento similar a la ejecución de la auditoría tradicional, el aporte de valor que debe trasladarse asociado a estos procesos radica en un incremento en la visibilidad sobre los riesgos de la organización, aunque ésta deba ser reforzada.

5.1.5.5. Retroalimentación.

En esta fase es donde se logra la mejora continua de los procesos de CA&CM, que se mejoran a partir de la información recopilada y las experiencias adquiridas durante la ejecución de la iteración actual. En ella, participará exclusivamente los roles que ejecutan CA&CM.

5.1.5.5.1. Subfases.

- ***5.1.5.5.1.1. Identificar puntos de mejora en los procesos CA&CM.***

Como resultado de las experiencias y problemas identificados por los miembros del equipo durante la ejecución de la iteración actual, deben identificarse y tratarse puntos de mejora en lo que respecta a la ejecución de los procesos de CA&M, cuando se considere que hay algún aspecto del modelo de ejecución que no esté aportando los resultados esperados.

5.1.5.5.1.2. Identificar puntos de mejora en los reportes de aseguramiento.

Puesto que la función de aseguramiento es crítica para dar visibilidad al Comité de Auditoría o al Consejo de Administración sobre los riesgos de la organización, y debe considerar las inquietudes y preocupaciones de todas las partes interesadas, deben analizarse los reportes emitidos y buscar puntos de mejora para que la comunicación con las partes interesadas sea más efectiva y eficiente.

5.1.5.5.1.3. Exponer puntos de mejora en las dinámicas de trabajo.

El último bloqueo de aspectos de mejora que debe identificarse es aquel asociado a la colaboración entre los miembros de auditoría interna que ejecutan CA&CM. En esta subfase el mánager o el responsable del aseguramiento debe debatir, de forma conjunta o individualizada, según se considere oportuno dependiendo de la situación, aquellas situaciones que se hayan producido en las dinámicas de colaboración entre los miembros y que hayan provocado problemas o enfrentamientos entre ellos.

Es fundamental que todas las cuestiones identificadas en esta sub-fase se resuelvan por parte del mánager de auditoría o del responsable del aseguramiento a la mayor brevedad, puesto que podrían llegar a tener un impacto significativo en la productividad y en el desarrollo de los procesos.

En esta subfase debe plantearse el trabajo como un proceso de identificación de puntos de mejora, sin hincapié en reproches o en los conflictos que se hayan producido, para que ésta no se vea como un punto de ataque a los miembros del grupo sino una forma de mejorar el ambiente de trabajo.

5.1.5.5.1.4. Definir objetivos de mejora internos.

Una vez expuestos todos los puntos sobre los que es necesario trabajar, se definirán objetivos de mejora que cumplirán las propiedades S.M.A.R.T. ya descritas en secciones previas, a fin de que puedan observarse de forma más clara las mejoras alcanzadas.

5.1.5.5.1.5. Incorporar elementos de mejora a la Lista de Tareas Pendientes.

Todos los elementos de mejora se irán identificando, y de entre todos ellos, a medida que se quieran ir trabajando, se irán incorporando en la lista de tareas pendientes. Estos aspectos, a la hora de ser incorporados a dicha lista, deberán definirse de la misma manera y contar con un nivel de detalle similar al del resto de las tareas.

5.1.5.5.1.6. Exponer los logros del proceso de CA&CM.

Es importante dar visibilidad a las mejoras en la función de aseguramiento fruto de la ejecución de procesos de CA&CM, para que el equipo sea consciente de ellas, y no solo de los aspectos a mejorar.

5.1.5.5.1.7. Exponer los logros del equipo.

De la misma manera que ocurre con la subfase anterior, también es vital que se expongan abiertamente, estando presentes todos los miembros del equipo, los logros alcanzados por el equipo, tratando aportar una visión de grupo en lugar de una individualizada.

5.1.5.5.2. Consideraciones.

Las consideraciones básicas a la hora de abordar esta fase son las siguientes:

- El tiempo destinado a esta fase es del 5% del tiempo de la iteración.
- Para que se logre una verdadera mejora continua, deben incluirse dentro de las siguientes iteraciones alguno de los elementos de mejora añadidos a la lista de tareas pendientes, aunque no existe un criterio fijo en lo que respecta a cuántos elementos de esta tipología incorporar. Puesto que estos elementos también se encuentran cuantificados y priorizados en la lista de tareas pendientes, dicha priorización puede utilizarse como criterio para su incorporación en las iteraciones. Se podrá llegar a la conclusión de que un punto de mejora debe introducirse de forma urgente en la lista de tareas pendientes cuando dicho aspecto se identifique repetidamente en las iteraciones posteriores.
- Existe una salvedad a la hora de incorporar puntos de mejora a la lista de tareas pendientes, y son aquellos que impacten en las relaciones entre equipo, que deberán ser gestionados directamente, y requerir la involucración solo de aquellos miembros involucrados de forma directa.
- Es responsabilidad del mánager de auditoría obtener la información relevante para la mejora de los procesos, si bien el responsable del aseguramiento debe participar en el diseño de las mejoras que resulte necesario introducir, y es el responsable de priorizar su aplicación.
- El perfil a cargo de identificar puntos de mejora, especialmente aquellos que afecten a las dinámicas de grupo, debe contar con habilidades interpersonales robustas, puesto que de otra manera el equipo y los procesos de CA&CM pueden salir perjudicados.

5.1.5.6. Refinamiento.

Esta fase es opcional, y puede llevarse a cabo en cualquier momento de la iteración, especialmente cuando se hayan finalizado todas las tareas de la lista de iteración, puesto que ayudará a reducir el tiempo necesario para la siguiente fase de planificación.

5.1.5.6.1. Subfases.

- ***5.1.5.6.1.1. Exposición de las tareas incorporadas a la Lista de Tareas Pendientes.***

El responsable del aseguramiento o el mánager de auditoría debe exponer al equipo de auditoría las tareas incorporadas a la lista de tareas pendientes.

Esta exposición se debería centrar en las tareas que han sido añadidas a lo largo de la iteración en curso, puesto que el equipo de auditoría aún no tiene información detallada sobre ellas; y en aquellas tareas que han sido descartadas para su inclusión en la lista de iteración, dado que este hecho supondrá la necesidad de rediseñar o incrementar el nivel de detalle la tarea, y hacerlo en esta fase ayuda a aligerar la siguiente pase de planificación cuando no haya otras tareas que ejecutar.

- ***5.1.5.6.1.2. Aclaración de dudas sobre las tareas.***

Tras la exposición de las tareas, el equipo de auditoría expondrá todas las dudas que le surjan y que les impidan entenderla hasta el punto de no poder incorporarla a la lista de iteración. Por su parte, el responsable del aseguramiento o el mánager de auditoría deberán desarrollar las tareas para dar respuesta a las dudas planteadas por el equipo de auditoría.

- ***5.1.5.6.1.3. Modificación de las tareas en la lista de tareas pendientes.***

Una vez realizadas las aclaraciones oportunas al equipo de auditoría, y cuando todos los roles tengan una visión común sobre una tarea y se sientan confortables con su desarrollo, ésta se modificará en la lista de tareas pendientes para reflejar las modificaciones y aclaraciones realizadas durante el refinamiento.

5.1.5.6.2. Consideraciones.

Las consideraciones básicas a la hora de abordar esta fase son las siguientes:

- No existe un tiempo límite fijado para esta fase, pero el volumen dedicado sobre el total de la iteración debería mantenerse siempre bajo o muy bajo (inferior al 5%), y ejecutarse

siempre consumiendo el tiempo de la fase de ejecución, una vez que se hayan acabado las tareas a ejecutar en la iteración.

- Debe centrarse en aquellas tareas que hayan sido descartadas, para asegurar que no se vuelven a descartar en la siguiente fase de planificación, aunque puede incluir nuevas tareas que se consideren especialmente complejas.

- Esta fase requiere la involucración de todo el equipo.

5.2. Modelo incremental de madurez.

A medida que se vayan ejecutando iteraciones de los procesos de CA&CM, se irá incrementando su madurez, así como la agilidad del equipo encargado de su ejecución. En este proceso, existen 4 niveles básicos de madurez por los que irán evolucionando los procesos de CA&CM.

Estos niveles de madurez requerirán la introducción de modificaciones sobre las fases de la iteración, tal y como se describe a continuación.

5.2.1. Inicial.

Durante la etapa inicial de madurez, el equipo aún se está familiarizando con la ejecución de procesos de CA&CM, y el número de elementos clave supervisados es reducido, por lo que los procesos de CA&CM aún no resultarán eficientes, y no se dispondrá de suficiente información como para introducir mejoras sustanciales en dichos procesos

Los modificadores de este nivel sobre las fases de la iteración son los siguientes:

- Se incrementa el porcentaje de dedicación a la fase de planificación, asegurando que se definan de forma adecuada tanto las tareas y subtareas, como los elementos clave de supervisión.

- Los reportes fruto de la ejecución de los procesos de CA&CM no se elevan a las partes interesadas hasta haber sido contrastados con fuentes alternativas y mediante la ejecución de sucesivas iteraciones.

- La supervisión del responsable del aseguramiento debe ser más estrecha, para mejorar el alineamiento entre los requerimientos del negocio y los objetivos de los procesos de CA&CM.

- Debe reforzarse la transparencia con las partes interesadas para que durante este nivel se obtenga feedback con mayor frecuencia, y poder construir los procesos sobre principios alineados con sus necesidades.

- Es recomendable centrar la incorporación de elementos clave que cubran los riesgos de mayor criticidad para la organización.

- Deben introducirse algunos elementos clave de supervisión sobre el servicio cloud, priorizando aquellos de menor impacto, para que el equipo adquiera experiencia supervisando este entorno, y seleccionando a nivel interno los elementos de supervisión más representativos para el análisis de recursos tecnológicos desplegados on premise, sobre los que resultará más sencillo obtener feedback.

- En este nivel, es preferible no comunicar los resultados de los procesos a partes interesadas externas a la organización.

5.2.2. Expansión horizontal – Acoplamiento.

La expansión de los procesos CA&CM tiene dos dimensiones principales. En primer lugar, se irán introduciendo nuevos elementos clave en el flujo de iteración. En segundo lugar, se incrementarán los recursos y procesos sobre los que usar CA&CM como estrategia de supervisión.

La introducción paulatina de elementos clave en el modelo ayudará a identificar sinergias o puntos de mejora entre ellos, al mismo tiempo que empezará a ofrecer resultados de mayor calidad, pudiendo detectar la causa de los fallos que se detecten en el proceso mediante el análisis de las iteraciones previas y sus resultados.

El incremento en el alcance de los recursos tecnológicos a supervisar aumentará el volumen de información resultante de la ejecución del proceso de forma gradual, favoreciendo que se establezcan y depuren las estructuras de reporte necesarias para la comunicación de resultados. Además, el incremento gradual de alcance permitirá que aquellos aspectos que resulte necesario corregir en fases tempranas de la ejecución se resuelvan antes de que se apliquen los procesos de CA&CM sobre un número mayor de recursos, reduciendo así el coste de ejecutar correcciones.

El cambio a este nivel de madurez deberá producirse una vez que el equipo haya adquirido un nivel de conocimiento básico sobre los procesos, de forma que se sienta cómodo en su ejecu-

ción, y tras haber identificado y corregido aquellos aspectos más significativos producto de la falta de experiencia de la organización y de la función de auditoría interna de TI ejecutando CA&CM.

Los modificadores de este nivel sobre las fases de la iteración son los siguientes:

- La implantación de elementos clave de supervisión debe realizarse de forma agrupada, de tal modo que no se incorporen elementos aislados, sino que la integración de éstos producida en una iteración permita obtener resultados fiables sobre los nuevos riesgos o recursos considerados. Estas agrupaciones deben considerarse a nivel de riesgo, recurso o dominio de control.

- Deben empezar a integrarse en los procesos de CA&CM riesgos y elementos clave de supervisión asociados a recursos externalizados, para iniciar una ampliación de la visibilidad del riesgo para la organización fuera de los límites de ésta.

- Conviene realizar una identificación periódica de nuevas partes interesadas, que hayan podido surgir al incrementar el alcance de los procesos de CA&CM.
  Es conveniente que el responsable del aseguramiento o el mánager de auditoría refuercen sus labores de asesoramiento a las áreas, les ayuden a entender y contextualizar los resultados obtenidos por estos procesos, y recaben su feedback de manera frecuente.

- Es importante analizar los resultados de la ejecución de los procesos comparándolos con iteraciones previas, para detectar cualquier aspecto anómalo que pueda indicar una incorrecta integración de un elemento clave de supervisión o de un recurso en los procesos.

- El tiempo dedicado a la fase de planificación debe empezar a reducirse, en favor del tiempo dedicado a la fase de ejecución.

5.2.3. Expansión vertical – Maduración.

La maduración de los procesos de CA&CM requiere un enfoque mucho mayor en el aporte de valor de éstos al aseguramiento de la organización. Una vez que estos procesos cubren un número suficiente de recursos y en su iteración se gestionan suficientes elementos clave de supervisión como para que los resultados reportados ofrezcan información relevante y de valor, es el momento de prestar mayor atención al análisis de dichos resultados, y a su integración con otros procesos y reportes de la función de aseguramiento.

Es en este nivel de madurez cuando la función de auditoría interna puede centrarse con mayor detalle en satisfacer los objetivos globales asociados a los procesos de CA&CM, y en mejorar el alineamiento entre la información obtenida tras la ejecución de los procesos con las expectativas de las partes interesadas.

Debe perseguirse este nivel de madurez una vez que los procesos de CA&CM cubran suficientes elementos clave de supervisión como para que los resultados obtenidos sean integrables en otras fuentes de reporte o procesos de aseguramiento. Podrá buscarse este nivel de madurez incluso aunque no se haya completado la extensión completa de los procesos sobre todos los recursos tecnológicos o sin haber integrado todos los elementos clave de supervisión, dado que es preferible tratar de mejorar los resultados del proceso al mismo tiempo que se integran los últimos recursos y elementos clave de supervisión.

Los modificadores de este nivel sobre las fases de la iteración son los siguientes:

- Debe continuarse reduciendo paulatinamente el tiempo dedicado a la planificación hasta conseguir que ocupe un 5%-10% del tiempo total de la iteración.

- Los reportes generados como resultado de la ejecución de los procesos de CA&CM deben ser evaluados frecuentemente, identificar aquellos aspectos relevantes para las partes interesadas o para los procesos en los que se integrarán y que no hayan sido incorporados, y depurarlos para que ofrezcan la información de mayor calidad y relevancia disponible para las partes interesada o para el proceso al que se destinan.

- Debe prestarse atención a la fase de retroalimentación, para que haya una incorporación frecuente a la lista de tareas pendientes de aspectos de mejora.

- Debería lograrse una reducción en el número de nuevos elementos clave de supervisión a integrar, e incrementarse el número de elementos ya integrados supervisados o mejorados, de forma que se incremente la consistencia en los resultados entre iteraciones.

- En este nivel, los resultados de la ejecución de CA&CM deben alimentar los procesos de auditoría, y éstos deberían usarse de soporte en las fases de evaluación preliminar, elaboración del programa de trabajo, y de forma complementaria durante el desarrollo del trabajo de campo.

5.2.4. Consolidación.

Una vez alcanzado este nivel de madurez, los procesos de CA&CM se verán sujetos a una verdadera mejora continua, mediante el análisis y depuración de los procesos de CA&CM y de los elementos clave analizados durante su ejecución. Al mismo tiempo, puesto que los procesos ya son suficientemente maduros y éstos aportan valor a la organización, el objetivo principal de esta fase es conseguir mantener dicho aporte de valor a lo largo del tiempo, adaptando los procesos de CA&CM a medida que los requerimientos de aseguramiento y de negocio lo vayan requiriendo.

En este nivel, aún será necesario realizar modificaciones sobre elementos clave de supervisión, puesto que podrían identificarse elementos de supervisión más eficientes, preciosos, o que respondan mejor a los cambios en el contexto interno o externo de la organización.

El cambio a este nivel de madurez se debe producir una vez que el equipo que ejecuta los procesos de CA&CM estime que se ha obtenido un nivel de aporte de valor a la organización razonable, y que se posee un conocimiento consolidado sobre la ejecución de los procesos de CA&CM y sobre los riesgos supervisados mediante la ejecución de dichos procesos.

Los modificadores de este nivel sobre las fases de la iteración son los siguientes:

- El responsable del aseguramiento identifica e introduce en la pila de tareas pendientes aquellos elementos para conseguir que los procesos de CA&CM evolucionen en la misma dirección que la organización.
- Se vuelven a introducir elementos clave de supervisión en la matriz de integración, que suponen una optimización de los existentes, o que permiten la sustitución de elementos poco maduros por otros más eficientes.
- El tiempo dedicado a la fase de planificación debe mantenerse al mínimo, no superando un 5%-10% del tiempo total de la iteración.
- Los elementos clave de supervisión desplegados deberían ofrecer un nivel de visibilidad sobre el servicio cloud homogéneo con respecto a la visibilidad ofrecida sobre los recursos internos.
- Los resultados obtenidos fruto de la ejecución de los procesos de CA&CM deben ali-

- mentar los procesos de selección de nuevos servicios cloud, y de renegociación o análisis de los existentes.

- El nivel de automatización de análisis de elementos clave de supervisión debe ser el máximo permitido por la tipología y características de cada uno de los elementos, así como por los recursos sobre los que éstos se despliegan.

- La elaboración de reportes para las partes interesadas y para su integración en otros procesos de aseguramiento debe estar total o parcialmente automatizada, y ser revisada periódicamente en busca de puntos de mejora y necesidad de adaptación.

5.3. Nivel de integración en la función de aseguramiento.

Los procesos de CA&CM están diseñados para ofrecer aseguramiento a la organización y visibilidad sobre los riesgos a los que ésta se ve expuesta. Por tanto, dichos procesos pueden resultar beneficiosos para la función de auditoría interna de una organización.

Existen diversos enfoques a la hora de plantear la integración de los procesos de CA&CM con otros procesos encargados de la supervisión del riesgo de la organización.

5.3.1. Ejecución completamente integrada con la función de auditoría interna.

La ejecución completamente integrada implica la sustitución de los procesos de aseguramiento tradicionales basados en la ejecución de auditorías por la ejecución de los procesos de CA&CM como única fuente de aseguramiento de la organización.

5.3.1.1. Pros.

- Puede aportar niveles básicos de aseguramiento en organizaciones poco maduras que no posean los recursos para desarrollar una función de auditoría interna completa.

- Puede cubrir un alcance mayor que un enfoque de auditoría tradicional.

- Si la organización hace uso de principios ágiles de gestión, permite una mejor integración con el resto de los procesos de la organización y su modo de operar.

5.3.1.2. Contras.

- El nivel de aseguramiento es en general inferior a aquel obtenido mediante la ejecución de auditorías tradicionales, en lo que respecta a la profundidad del análisis.
- Resulta complejo dar respuesta a las inquietudes de los órganos de control y gobierno basándose exclusivamente en procesos CA&CM.
- Resulta más complejo abstraer conocimiento de los resultados de la medición obtenidos en comparación con las auditorías tradicionales.

5.3.2. Ejecución disociada de la función de auditoría interna.

El resultado de la ejecución de los procesos de CA&CM no se integra en la función de auditoría interna, y por tanto se obtienen reportes independientes que no se llegan a integrar en ningún momento.

En este enfoque, los procesos de CA&CM pueden ser ejecutados por la función de auditoría interna o por cualquier otra función de gestión del riesgo, como la función de ciberseguridad.

5.3.2.1. Pros.

- La ejecución de CA&CM aporta un valor extra a la ejecución de auditorías, sin comprometer la calidad de éstas.
- Se elimina la necesidad de coordinar la ejecución de CA&CM y las auditorías tradicionales, lo que reduce la complejidad en su aplicación.

5.3.2.2. Contras.

- No se obtienen sinergias en la ejecución de los procesos de forma conjunta.
- El número de recursos requerido para la ejecución de ambas tipologías de procesos es muy superior al del resto de enfoques.
- Puede generar confusión e inseguridad en caso de que las conclusiones obtenidas mediante la ejecución de auditorías y de CA&CM posean discrepancias.

5.3.3. Integración balanceada con la función de aseguramiento.

Este nivel de integración comprende la ejecución de los procesos de CA&CM por parte de la función de auditoría interna, de forma que los resultados obtenidos por éstos alimenten la ejecución de auditorías.

La integración balanceada es el modelo propuesto en el presente documento, al considerar que ofrece un mejor equilibrio y resultados a la función de auditoría interna.

5.3.3.1. Pros.

- Se logra una optimización clara de la función de auditoría, obteniendo una visión general de los riesgos de la organización mediante CA&CM, que es complementada con análisis de mayor profundidad sobre aspectos críticos mediante la ejecución de auditorías.

- Se trata de un enfoque flexible que permite el contraste de resultados por parte de la función de auditoría interna, pudiendo adaptar de forma ágil las fuentes para el reporte.

- Ofrece una mayor profundidad en el análisis de los riesgos, al aportar visiones complementarias, con un alcance completo gracias a CA&CM y de gran profundidad gracias a la ejecución de auditorías.

5.3.3.2. Contras.

- Este enfoque requiere el uso de un número elevado de recursos, puesto que además de la ejecución de los procesos de CA&CM, los equipos de auditoría deben continuar ejecutando auditorías como lo venían haciendo antes de integrar CA&CM.

- Existe cierta complejidad a la hora de encontrar un punto de integración óptimo de forma que CA&CM aporte valor al proceso de auditoría sin llegar a entorpecerlo.

CONCLUSIONES 6

Como resultado del trabajo desarrollado a lo largo del presente documento, se han alcanzado las conclusiones que se exponen a continuación.

6.1. Aporte de valor a la función de auditoría interna de TI.

El aporte de valor de CA&CM a la función de aseguramiento de la organización es mayor que si no se ejecutan estos procesos, y su aplicación incrementará la eficiencia y eficacia de la función de auditoría interna de TI. Sin embargo, debe encontrarse la configuración óptima para su ejecución, a partir de las características y requerimientos de la organización y de la función de auditoría de TI. Dicha configuración se gestionará principalmente mediante la selección de los elementos clave de supervisión que se integrarán en CA&CM, la selección del grado de automatización de los procesos, el modelo de integración entre CA&CM y los procesos de aseguramiento tradicionales, y el uso que se haga de la información reportada por CA&CM.

6.2. Viabilidad de la solución propuesta.

Puesto que la eficacia y la eficiencia de integrar CA&CM con la función de auditoría interna de TI se logrará solo bajo determinadas circunstancias, es importante llevar a cabo un análisis formalizado sobre la aplicabilidad y beneficios esperados del modelo propuesto sobre la organización sobre la que se pretende implementar. Una vez realizado este análisis, solo deberá integrarse CA&CM con la función de auditoría interna de TI cuando la solución resulte costo-efectiva, y aporte beneficios claros a la organización.

6.3. Nivel de integración.

La integración de procesos de CA&CM resulta más sencilla y efectiva cuando se combina con la ejecución de auditorías tradicionales, puesto que las sinergias entre ambas son elevadas, y su ejecución conjunta permite eliminar ciertas limitaciones presentes en ambos modelos de aseguramiento. Por su parte, utilizar exclusivamente CA&CM para ofrecer aseguramiento no siempre producirá resultados con el nivel de detalle requerido.

6.4. Visión completa y consistente.

Si bien deben evaluarse todos los ecosistemas tecnológicos de la organización sobre la que se implementa CA&CM, debe ofrecerse una visión total y consistente de los riesgos. Por tanto, los reportes generados como resultado de la ejecución de los procesos de CA&CM deben ofrecer una visión completa de los riesgos para que aporte el máximo valor a la organización. Además, deben integrar el análisis de información, controles y riesgos, para acabar concluyendo sobre la exposición de la organización al riesgo tecnológico de la organización, independientemente de que sobre el resultado general se aporten conclusiones complementarias más desagregadas.

6.5. Homogeneización de la supervisión de recursos cloud.

El uso de CA&CM, por la abstracción que logran los resultados de los recursos tecnológicos evaluados, permite una mejor integración de las actividades de supervisión de recursos cloud con el resto de las actividades de aseguramiento. Esta abstracción no es inmediata, y deberá lograrse mediante la definición de elementos clave de supervisión que permitan la realización de evaluaciones homogéneas sobre los recursos tecnológicos independientemente de su arquitectura.

6.6. Interacción con el CSP.

Aunque el aporte de valor a la organización resulte mayor al usar CA&CM sobre servicios cloud, también se generan mayores requerimientos de provisión de información procedente de la infraestructura subyacente al servicio, lo que debe ser gestionado a nivel contractual con el CSP, y puede introducir dificultades a la hora de obtener su compromiso.

6.7. Evolución del modelo de supervisión.

Un aspecto fundamental logrado con el modelo de supervisión propuesto es la capacidad para extender la función de aseguramiento fuera de los límites de la organización. Dado que, cada vez más, las organizaciones se configuran en cadenas de valor extendidas que soportan la interrelación entidades mediante la tecnología, disponer de un modelo de supervisión efectivo para la evaluación del riesgo en recursos externalizados y que sea extrapolable a diversos modelos de externalización es fundamental para ofrecer aseguramiento al Comité de Auditoría y a la Dirección.

6.8. Requerimientos de adaptación.

Un aspecto clave de los procesos de CA&CM son los elementos clave de supervisión que deben seleccionarse y evaluarse para poder obtener resultados relativos a la calidad de los datos, la eficacia de los controles y los riesgos de la organización. Aunque existen marcos de controles, mapas de riesgos y ejemplos de KPIs y KRIs disponibles para su consulta, estos elementos deben seleccionarse cuidadosamente para que den respuesta a las necesidades de supervisión de cada organización. Además, deben ser adaptados para que los resultados obtenidos fruto de su análisis sean representativos para la organización. A este respecto, aunque se pueden definir conjuntos estándar de elementos clave de supervisión, cada organización debe dedicar recursos a la definición o adaptación de estos elementos de supervisión hasta obtener un conjunto propio que permita una supervisión efectiva y eficiente a partir de sus características particulares.

6.9. Mantener un enfoque consistente a lo largo del tiempo.

Aunque pueden introducirse cambios sobre los procesos que forman CA&CM, e incluso considerarse que, pasado un tiempo, la ejecución de estos procesos no está aportando valor a la organización y optarse por un enfoque de auditoría que prescinda de ellos, mientras se decida mantener la ejecución de CA&CM, deben respetarse los principios de CA&CM y perseguir los objetivos fijados en todo momento. Introducir cambios frecuentes y sin una motivación clara evitará que se consigan los resultados esperados, y no se llegará a permitir la introducción de un ciclo de mejora continua basado en la iteración y la depuración del modelo.

6.10. Madurez frente a sencillez

Queda claro que ofrecer aseguramiento haciendo uso de CA&CM y de la ejecución de auditorías tradicionales introduce mucha más complejidad sobre la supervisión, independientemente de los beneficios que se obtengan. Aunque tratar de mantener los procesos lo más simples posible es una buena práctica de gestión, conviene tener presente que lograr un incremento en la madurez de la supervisión e incrementar el aporte de valor requiere la introducción de cierta complejidad sobre los procesos. En ese sentido, el modelo de supervisión desarrollado en el presente documento no tiene por objetivo simplificar el proceso de auditoría, sino lograr su integración en un contexto organizacional y tecnológico complejos para ofrecer un mayor aseguramiento, y por ello debe renunciar en cierto grado a la simplicidad en favor de la eficacia de la supervisión, sin que ello implique descuidar la eficiencia de los procesos desarrollados.

Anexo A: Objetivos de control cloud

A.1. Cumplimiento y supervisión.

A.1.1. Objetivo de control general.

Este dominio de controles garantiza el cumplimiento con los requerimientos legales aplicable a la gestión de la tecnología y la ciberseguridad, además de asegurar un adecuado nivel de control y supervisión sobre los recursos tecnológicos.

A.1.2. Objetivos de control enfocados en el servicio cloud.

- OC.CYS.1 – La organización debe ser consciente de las obligaciones de cumplimiento asociadas al servicio en la nube contratado, tanto por su parte como por la del CSP, y asegurar que los requerimientos regulatorios se tienen en cuenta a la hora de diseñar el modelo de gobierno del servicio cloud.
- OC.CYS.2 – Asegurar la cobertura de los principales riesgos tecnológicos para la organización dentro del plan anual de auditoría, en el que se incluya supervisión de entornos cloud, en la medida en la que éstos se vean sujetos a dichos riesgos y según la importancia del servicio para la organización.
- OC.CYS.3 – Garantizar que la organización, y en especial los órganos de gobierno y control, poseen información suficiente sobre el servicio cloud y los riesgos asociados a éste como para que la toma de decisiones no se vea afectada negativamente.

A.2. Gestión del riesgo.

A.2.1. Objetivo de control general.

Los controles dentro de este dominio de control aseguran una adecuada gestión de los riesgos tecnológicos, mediante la identificación de todas las fuentes de información relevantes y una gestión que se adapte a los cambios organizativos a lo largo del tiempo.

A.2.2. Objetivos de control enfocados en el servicio cloud.

- OC.GDR.1 – Los riesgos tecnológicos y de cumplimiento asociados al servicio cloud debe integrarse en el sistema de gestión del riesgo de la organización, y éstos deben ser evaluados para poder priorizar correctamente la gestión de dichos riesgos.
- OC.GDR.2 – Se han tenido en cuenta todos los condicionantes internos y externos tanto para el cliente del servicio como para el CSP a la hora de identificar y evaluar los riesgos asociados al servicio cloud, lo que permite que dicho proceso considere cualquier aspecto relevante para dichos riesgos.
- OC.GDR.3 – El análisis de riesgos del servicio cloud se mantiene actualizado, considerando cualquier cambio relevante los procesos soportados por el servicio, en la infraestructura tecnológica de soporte, y en los datos gestionados por dicho servicio.

A.3. Privacidad.

A.3.1. Objetivo de control general.

Los controles de privacidad protegen los datos personales y su uso dentro de la organización, y velan por que éstos permanezcan seguros durante todo su ciclo de vida, incluyendo su gestión por terceros.

A.3.2. Objetivos de control enfocados en el servicio cloud.

- OC.PRI.1 – Asegurar que la privacidad de la información personal y sensible de la organización se tiene en cuenta a lo largo de todo el ciclo de vida de la gestión del servicio cloud.
- OC.PR.2 – Garantizar la seguridad de los datos personales gestionados en el entorno cloud a lo largo de todo el ciclo de vida de la información, incluyendo su adquisición, tratamiento, almacenamiento, envío y destrucción.
- OC.PR.3 – Obtener aseguramiento a lo largo del tiempo respecto al cumplimiento del CSP de los requerimientos en materia de privacidad.

A.4. Gobierno y protección del dato.

A.4.1. Objetivo de control general.

Asegurar el gobierno y protección de los datos utilizados por la organización mediante la implantación de controles garantizará que éstos permanecen bajo control, y que no se producirá un deterioro en las operaciones o un impacto adverso para la organización fruto de un decremento en la calidad de la información gestionada.

A.4.2. Objetivos de control enfocados en el servicio cloud.

- OC.GPD.1 – Garantizar que todos los datos que soportan procesos críticos de la organización, incluyendo los procesos que hacen uso de los servicios cloud contratados, están correctamente identificados, y tienen un responsable asignado con suficientes recursos y autoridad como para facilitar la toma de decisiones sobre éstos para asegurar su protección.
- OC.GDP.2 – Asegurar que la calidad de los datos, incluso cuando éstos sean almacenados o gestionados en un entorno cloud, se mantiene en niveles aceptables para soportar los procesos de negocio.
- OC.GDP.3 – Lograr que los datos sensibles para la organización permanecen protegidos tanto cuando se encuentren almacenados y sean gestionados dentro de la propia organización, como cuando sean gestionados o almacenados por servicios en la nube.

A.5. Continuidad.

A.5.1. Objetivo de control general.

Los controles destinados a salvaguardar la continuidad del negocio garantizan que, ante la ocurrencia de una contingencia, los recursos tecnológicos así como la propia organización, son capaces de recuperarse con el mínimo impacto posible sobre su funcionamiento.

A.5.2. Objetivos de control enfocados en el servicio cloud.

- OC.CON.1 – Los servicios cloud son tenidos en cuenta a la hora de diseñar los planes de continuidad y de recuperación corporativos, en la medida en la que dichos servicios soporten procesos críticos de la organización.
- OC.CON.2 – Asegurar que en el acuerdo firmado con el CSP se tienen en cuenta aspectos de la continuidad, en caso de que los servicios en la nube se incluyan como parte de la respuesta ante una contingencia, o que el servicio provisto por éstos se considere crítico.
- OC.CON.3 – Se han definido suficientes medidas de continuidad sobre el entorno cloud alineados con los requerimientos de continuidad para el servicio.

A.6. Gestión del cambio y mantenimiento de sistemas.

A.6.1. Objetivo de control general.

Este dominio de controles permite mantener la estrategia y recursos de TI con el negocio y sus objetivos a lo largo del tiempo, cubriendo uno de los aspectos clave del ciclo de vida de la tecnología como es su desarrollo o adquisición.

A.6.2. Objetivos de control enfocados en el servicio cloud.

- OC.GCM.1 – Las políticas y procedimientos de adquisición y desarrollo de sistemas tienen en cuenta las particularidades de los servicios cloud y del desarrollo en plataformas en la nube, para asegurar el alineamiento entre los requerimientos generales de la organización en cuanto a desarrollo de software y las capacidades de los servicios en la nube.
- OC.GCM.2 – Garantizar que todos los cambios que se produzcan sobre el servicio cloud y sobre la infraestructura subyacente que lo soporta son conocidos por la organización, y están controlados, siempre que éstos pudieran impactar adversamente sobre el servicio.
- OC.GCM.3 – Los cambios en el servicio cloud o en cualquier componente utilizado para prestarlo se gestionan de forma segura, por el cliente, el CSP, o mediante la coordinación de ambos.

A.7. Gestión operativa.

A.7.1. Objetivo de control general.

Si bien la tecnología suele servir de soporte a las operaciones de negocio, también es importante implantar controles que aseguren la propia operación de la tecnología, y que dicha operación sea consistente a lo largo del tiempo y tenga en cuenta buenas prácticas de seguridad.

A.7.2. Objetivos de control enfocados en el servicio cloud.

- OC.GOP.1 – El uso de los servicios cloud cuenta con procedimientos de soporte suficientes como para asegurar que la operativa es consistente a lo largo del tiempo, y que ésta no se degrada por falta de control o conocimiento sobre ésta.
- OC.GOP.2 – La operación de procesos soportados por servicios cloud debe realizarse teniendo en cuenta principios de seguridad, y dichos principios deberán considerar todos los recursos tecnológicos de soporte al proceso.

A.8. Interoperabilidad y Portabilidad.

A.8.1. Objetivo de control general.

En un contexto cada vez más cambiante y con un número creciente de proveedores involucrados en la gestión u operación de la tecnología, es importante que existan controles que faciliten al máximo las transiciones o migraciones tecnológicas que se produzca en la organización.

A.8.2. Objetivos de control enfocados en el servicio cloud.

- OC.IYP.1 – En el momento en el que se opta por contratar servicios en la nube, como ocurre con cualquier otro recurso tecnológico, deberán adoptarse medidas que garanticen que no

se produce un bloqueo causado por dicha adopción, comúnmente conocido como vendor lock-in.

- OC.IYP.2 – El uso de cualquier tecnología, incluyendo tecnología cloud, deberá permitir la interconexión con el resto de los componentes tecnológicos mediante sistemas de comunicación o intercambio de información estandarizados.
- OC.IYP.3 – Garantizar que la transición entre proveedores tecnológicos se produce de forma que genere el menor impacto posible en los procesos de negocio soportados por el proveedor, y que se cuenta con el soporte de éste durante el proceso para aquellas actividades que queden fuera del alcance del cliente.

A.9. Gobierno de ciberseguridad.

A.9.1. Objetivo de control general.

El dominio de controles destinado a asegurar un adecuado gobierno de ciberseguridad debe garantizar un correcto diseño estratégico de ésta, dotando al proceso de gestión de ciberseguridad de recursos, alineándolo con las necesidades y objetivos de la organización, y asegurando que toda gestión de los riesgos tecnológicos está estandarizada y responde a un propósito común.

A.9.2. Objetivos de control enfocados en el servicio cloud.

- OC.GDC.1 – Garantizar que durante el diseño del modelo de gobierno de la ciberseguridad se tiene en cuenta los riesgos, requerimientos y características de los servicios en la nube adquiridos.
- OC.GDC.2 – Asegurar que se han asignado responsabilidades sobre la protección del servicio en la nube y que las personas responsables poseen suficientes recursos, autoridad y conocimientos como para asegurar la adecuada protección del servicio.
- OC.GDC.3 – Las políticas, estándares, procedimientos, y demás documentación técnica, utilizada en la organización para asegurar una adecuada gestión de la ciberseguridad tienen en cuenta los servicios en la nube adquiridos, y se adaptan a estos para ofrecer niveles de protección similares a aquellos ofrecidos sobre tecnología propiedad de la organización.

A.10. Control de acceso.

A.10.1. Objetivo de control general.

El objetivo de este dominio es garantizar que únicamente los usuarios previamente autorizados y con una necesidad legítima pueden acceder a los recursos tecnológicos de la organización, y que dichos accesos respetan unos principios mínimos de seguridad.

A.10.2. Objetivos de control enfocados en el servicio cloud

- OC.CAC.01 – El entorno cloud es accedido únicamente por personal autorizado del cliente, de acuerdo con las funciones asignadas a cada rol, sin que su mayor exposición en Internet permita a un usuario no autorizado acceder a dicho entorno.
- OC.CAC.02 – Existen vías alternativas para el acceso al servicio cloud y a las funcionalidades de administración del mismo, de forma que un usuario no pueda ganar acceso privilegiado desde su vía de acceso predefinida.
- OC.CAC.03 – Las cuentas de usuario se gestionan de forma centralizada, de forma que los requerimientos de identificación, autorización y autenticación se mantiene consistente a lo largo de la organización, independientemente del ecosistema tecnológico al que se acceda.

A.11. Protección de la infraestructura tecnológica.

A.11.1. Objetivo de control general.

Este conjunto de controles asegura que la infraestructura tecnológica, a lo largo de todas sus capas, cuente con medidas de seguridad que minimicen la ocurrencia de riesgos de TI, incluyendo la protección de elementos propios de la infraestructura cloud.

A.11.1. Objetivo de control general.

- OC.PIT.01 – Asegurar que la infraestructura tecnológica bajo el control del cliente del servicio utilizada para su prestación cuenta con medidas de seguridad desplegadas que reducen la probabilidad o el impacto de la materialización de riesgos tecnológicos.
- OC.PIT.01 – Garantizar que las capas de la infraestructura cloud gestionadas por el cliente cuenta con controles de seguridad que reducen la probabilidad o el impacto de la materialización de riesgos tecnológicos.
- OC.PIT.02 – Garantizar que el uso de servicios en la nube no introduce riesgos sobre la infraestructura on premise gestionada por el cliente derivados de la interconexión entre ambas.
- OC.PIT.03 – Las redes de comunicación utilizadas para conectar los sistemas de la organización con el servicio en la nube se protegen de forma que el nivel de seguridad sea similar, o lo más parecido posible, al ofrecido en las redes internas de la organización.

A.12. Monitorización y análisis de sistemas.

A.12.1. Objetivo de control general.

Los controles dentro de este dominio están pensados para garantizar una correcta supervisión de los recursos tecnológicos, lo que permitirá detectan eventos de seguridad y comportamientos anómalos, y favorecerá la identificación de riesgos tecnológicos materializados.

A.12.2. Objetivos de control enfocados en el servicio cloud.

- OC.MAS.01 – Se lleva a cabo una adecuada supervisión del servicio cloud, de forma que sea posible analizar la actividad de los usuarios y del sistema, y detectar posibles eventos de seguridad con impacto adverso en la organización usuaria del servicio.
- OC.MAS.02 – La capacidad de supervisión de eventos de seguridad de la organización se extiende a lo largo de todos los recursos en uso, incluyendo recursos tecnológicos propios y los servicios cloud adquiridos.
- OC.MAS.03 – En la medida de lo posible, se llevan a cabo pruebas de seguridad que permita identificar vulnerabilidades presentes en los sistemas para su posterior tratamiento preventivo.

A.13. Cifrado.

A.13.1. Objetivo de control general.

El objetivo de los controles de cifrado es garantizar la integridad y confidencialidad de la información sensible de la organización, evitando que una gestión o uso incorrecto de las técnicas y claves de cifrado impacte adversamente sobre la información.

A.13.2. Objetivos de control enfocados en el servicio cloud.

- OC.CIF.01 – La información sensible se almacena y transmite cifrada, independientemente del recurso en el que se almacene o entre los que se transmita, incluyendo aquella almacenada en recursos cloud.
- OC.CIF.02 – Las claves de cifrado, incluyendo aquellas utilizadas en los recursos cloud gestionados por el cliente del servicio, se gestionan y almacenan de forma segura, de forma que se evite un compromiso de éstas.

A.14. Gestión de incidentes de seguridad.

A.14.1. Objetivo de control general.

Estos controles asegurarán que la organización esté preparada para la ocurrencia de incidentes de seguridad, que existan los medios necesarios para responder a éstos de forma adecuada, y que se investigan convenientemente para evitar que vuelvan a ocurrir.

A.14.2. Objetivos de control enfocados en el servicio cloud.

- OC.GIS.01 – Garantizar que la preparación para dar respuesta a los incidentes de seguridad tiene en cuenta las características y necesidades de todos los entornos tecnológicos usados por la organización, incluyendo los servicios cloud adquiridos.

- OC.GIS.02 – La gestión de incidentes de seguridad se lleva a cabo a lo largo de todos los recursos tecnológicos de la organización, incluyendo los servicios cloud, de forma que cualquier incidente sea identificado, contenido, analizado y tratado de forma holística a la organización, cubriendo cualquier sistema sobre el que éste se produzca.
- OC.GIS.03 – Deberá analizarse la capacidad de respuesta a incidentes de seguridad del cliente sobre los recursos tecnológicos propios, sobre los servicios cloud adquiridos, y en lo que respecta a la capacidad de gestión conjunta con el CSP.

A.15. Gestión de la cadena de valor extendida.

A.15.1. Objetivo de control general.

Con la introducción de proveedores en la cadena de valor de las organizaciones surge la necesidad de llevar a cabo un control y gestión mayor de la tecnología utilizada para soportar esta relación, de forma que la externalización de un servicio o un proceso no entrañe un mayor riesgo para la organización.

A.15.2. Objetivos de control enfocados en el servicio cloud.

- OC.GCV.01 – Garantizar que los recursos tecnológicos utilizados a lo largo de la cadena de valor extendida del usuario de servicios cloud se controlan y salvaguardan, independientemente de si son recursos externos accedidos por el cliente, recursos propios accedidos por un tercero, o recursos propios de uso interno.
- OC.GCV.02 – Existen prácticas por parte del usuario del servicio cloud y de sus proveedores que aseguran la transparencia en el gobierno de la tecnología y la ciberseguridad aplicada sobre ésta por parte de cualquiera de los actores involucrados.
- OC.GCV.03 – Los recursos tecnológicos de terceros utilizados a lo largo de la cadena de valor, entre los que se incluyen los servicios cloud cuando ofrecen soporte a procesos críticos de negocio, cumplen con los requerimientos de la organización que hace uso de éstos, y que el proveedor ofrece medios suficientes para validar el cumplimiento de dichos requerimientos.

Anexo B: Mapeo entre dominios de control y dominios CCM y NIST

B.1. Cumplimiento y supervisión.

- Planificación de auditorías (AAC-01_CCMv3)
- Auditorías independientes (AAC-02_CCMv3)
- Contacto con las partes interesadas (SEF-01_CCMv3)
- Identificación de requerimientos regulatorios (AAC-03_CCMv3)
- Programa de cumplimiento (AR-1_NISTSP80053)
- Reporte a los órganos de gobierno y control (GRM-05_CCMv3)
- Supervisión de la gestión (GRM-03_CCMv3)

B.2. Gestión del riesgo.

- Sistema de Gestión del Riesgo (GRM-11_CCMv3)
- Política y procedimientos de gestión del riesgo (RA-1_NISTSP80053 posible agrupación con GRM-11)
- Identificación de contextos internos y externos al cliente y el proveedor (BCR-05 y añadido)
- Análisis de Riesgos (GRM-10_CCMv3)
- Gestión del cambio asociado al riesgo (GRM-08_CCMv3)

B.3. Privacidad.

- Acuerdos de confidencialidad (HRS-07 y STA-05_CCMv3)
- Control de los datos recopilados para uso de un proveedor o terceros (Añadido)
- Aislamiento de los datos del cliente (Añadido)
- Adquisición de datos personales (IP-1_NISTSP80053)
- Acceso a datos personales propios (IP-2_NISTSP80053)
- Corrección de datos personales (IP-3_NISTSP80053)

- Gestión de reclamaciones relativas a la privacidad de información personal (IP-04_NISTSP80053)
- Requerimientos de privacidad para proveedores (AR-3_NISTSP80053)
- Monitorización y auditoría de la privacidad (AR-4_NISTSP80053)
- Reportes relativos a la privacidad (AR-6_NISTSP80053)
- Privacy by design (AR-7_NISTSP80053)

B.4. Gobierno y protección del dato.

- Inventario de datos e identificación de flujos de información (DSI-02_CCMv3)
- Propiedad y administración de los datos (DSI-07_CCMv3)
- Clasificación de la información (DSI-01_CCMv3)
- Uso y etiquetado de la información (DSI-04_CCMv3)
- Prevención de fugas de información (DSI-05_CCMv3)
- Uso de datos productivos (DSI-06_CCMv3)
- Eliminación segura de información (DSI-08_CCMv3)
- Protección de los datos (AIS-04_CCMv3)
- Calidad de la información (DI-1_NISTSP80053, DI-2_NISTSP80053)
- Minimización de información personal (DM-1_NISTSP80053 y DM-3_NISTSP80053)

B.5. Continuidad.

- Programa de gestión de la continuidad (BCR-10_CCMv3) (Sustituir por sistema de gestión)
- Políticas y procedimientos de gestión de la continuidad (BCR-11_CCMv3)
- Planificación de la continuidad (BCR-01_CCMv3)
- Análisis de Impacto (BCR-09_CCMv3)
- Pruebas de continuidad del negocio (BCR-02_CCMv3)
- Entrenamiento en continuidad (CP-3)
- Continuidad de servicios y suministros (BCR-03_CCMv3)
- Política de retención de activos (BCR-12_CCMv3)
- Alineamiento entre los requerimientos de continuidad y el contexto de la organización (CP-5_NISTSP80053)

B.6. Gestión del cambio y mantenimiento de sistemas.

- Política y procedimientos de mantenimiento de sistemas (MA-1_NISTSP80053 y SA-1_NISTSP80053)
- Adquisición y nuevos desarrollos (CCC-01_CCMv3)

- Externalización de desarrollos (CCC-02_CCMv3)
- Asignación de recursos (SA-2_NISTSP80053)
- Pruebas de calidad (CCC-03_CCMv3)
- Control en la gestión de cambios (CCC-04_CCMv3 y añadida)
- Cambios en producción (CCC-05_CCMv3)
- Detección de cambios (IVS-02_CCMv3)
- Protección de los datos durante las migraciones (IVS-10_CCMv3)
- Restricciones en el acceso al código fuente (IAM-06_CCMv3)
- Gestión de cambios en entornos externalizados (MA-4_NISTSP80053)
- Segregación de funciones en los procesos de cambio (MA-5_NISTSP80053)
- Mantenimiento de los activos (BCR-07_CCMv3)
- Proceso, estándares y herramientas de desarrollo (SA-15_NISTSP80053 y SA-17_NISTSP80053)

B.7. Gestión operativa.

- Política y procedimientos de operación (BCR-11_CCMv3)
- Seguridad de la operación (PL-7_NISTSP80053)
- Gestión centralizada (PL-9_NISTSP80053)

B.8. Interoperabilidad y Portabilidad.

- Políticas y procedimientos de relación (IPY-03_CCMv3)
- Peticiones de información y datos (IPY-02_CCMv3 y añadida)
- Estandarización técnica (software, APIs y protocolos de red) (IPY-01_CCMv3, IPY-04_CCMv3 e IPY-05_CCMv3)
- Soporte a la migración (Añadido)

B.9. Gobierno de ciberseguridad.

- Programa de gestión de la seguridad de la información (GRM-04_CCMv3)
- Documentación operativa (BCR-04_CCMv3)
- Documentación de los sistemas de información (IVS-04_CCMv3 y SA-5_NISTSP80053)
- Soporte e involucración del negocio (GRM-05_CCMv3)
- Requerimientos mínimos de ciberseguridad (GRM-01_CCMv3)
- Política de seguridad de la información (GRM-06_CCMv3 y GRM-09_CCMv3)
- Cumplimiento de la política (GRM-07_CCMv3)
- Formación y concienciación (HRS-10_CCMv3)
- Conocimiento de la industria y benchmarking (HRS-05_CCMv3)

- Definición de roles y responsabilidades (HRS-08_CCMv3)
- Responsabilidades de los usuarios (HRS-11_CCMv3)
- Uso aceptable de la tecnología (HRS-09_CCMv3)
- Arquitectura de seguridad de la información (PL-8_NISTSP80053)

B.10. Control de acceso.

- Política y procedimientos de identificación, autenticación y control de acceso (IAM-02_CCMv3, IAM-04_CCMv3, IA-1_NISTSP80053)
- Requerimientos de acceso de los clientes (AIS-02_CCMv3)
- Credenciales de usuarios (IAM-12_CCMv3)
- Uso de sistemas de autenticación robusta (SA-7_CCMv1)
- Autorización y restricciones de accesos de usuarios (IAM-09_CCMv3)
- Privilegios mínimos (IAM-08_CCMv3)
- Revocación de los derechos de acceso (IAM-11_CCMv3)
- Revisión de acceso de usuarios (IAM-10_CCMv3)
- Segregación de funciones (IAM-05_CCMv3)
- Acceso a herramientas de auditoría o administración (IAM-01_CCMv3)
- Acceso a puertos de diagnóstico o configuración (IAM-03_CCMv3)
- Acceso a utilidades de sistema (IAM-13_CCMv3)
- Interconexión entre sistemas (CA-3_NISTSP80053)
- Identificación y autenticación de dispositivos y servicios (IA-3_NISTSP80053, IA-9_NISTSP80053)
- Re-autenticación (IA-11_NISTSP80053)

B.11. Protección de la infraestructura tecnológica.

- Protección de las aplicaciones (AIS-01_CCMv3)
- Controles de Integridad (AIS-03_CCMv3)
- Segregación de entornos en el lado del cliente (IVS-08_CCMv3)
- Segregación de entornos multi-cliente (en el lado del proveedor) (IVS-09_CCMv3)
- Sincronización de relojes (IVS-03_CCMv3)
- Identificación automática de recursos (DCS-03_CCMv3)
- Código móvil (TVM-03_CCMv3)
- Protección de las redes (IVS-06_CCMv3)
- Integridad y confidencialidad de las transmisiones (SC-8_NISTSP80053 analizar posibilidad de fusionar con IV-06_CCMv3)
- Autenticidad de las sesiones (SC-23_NISTSP80053)
- Seguridad en redes inalámbricas (IVS-12_CCMv3)

- Gestión de redes compartidas (SA-11_CCMv1)
- Gestión de parches y vulnerabilidades (IVS-05_CCMv3, TVM-02_CCMv3, SI-2_NISTSP80053)
- Bastionado del sistema operativo (IVS-07_CCMv3)
- Bastionado del hipervisor (IVS-11_CCMv3)
- Protección frente a código malicioso (TVM-01_CCMv3)
- Gestión de la información en recursos compartidos (SC-4_NISTSP80053)
- Disponibilidad de la información (SC-5_NISTSP80053 y SC-6_NISTSP80053)
- Ocultamiento y balanceo (SC-30_NISTSP80053)
- Restricción y validación de los datos de entrada y salida (SI-9_NISTSP80053, SI-10_NISTSP80053, SI-11_NISTSP80053, SI-15_NISTSP80053)

B.12. Monitorización y análisis de sistemas.

- Gestión de logs (IVS-01_CCMv3)
- Análisis de amenazas persistentes en los sistemas (RA-6_NISTSP80053)
- Pentesting (CA-8_NISTSP80053)
- Monitorización de sistemas de información (SI-4_NISTSP80053)
- Gestión de alertas de seguridad (SI-5_NISTSP80053)
- Revisión de funcionalidades de seguridad (SI-6_NISTSP80053)

B.13. Cifrado.

- Cifrado de información sensible (EKM-03_CCMv3)
- Generación de claves de cifrado (EKM-02_CCMv3)
- Gestión de claves de cifrado (EKM-04_CCMv3)

B.14. Gestión de incidentes de seguridad.

- Política y procedimientos de gestión de incidentes de seguridad (SEF-02_CCMv3, IR-8_NISTSP80053)
- Preparaciones legales para la respuesta a incidentes (SEF-04_CCMv3)
- Entrenamiento para la respuesta a incidentes (IR-2_NISTSP80053)
- Comunicación de incidentes (SEF-03_CCMv3)
- Métricas de la respuesta ante incidentes (SEF-05_CCMv3)
- Monitorización de incidentes (IR-5_NISTSP80053)
- Reporte de incidentes (IR-6_NISTSP80053)

B.15. Gestión de la cadena de valor extendida.

- Protección de la cadena de suministro (SA-12_NISTSP80053)
- Transparencia y responsabilidad (STA-01_CCMv3, STA-02_CCMv3 y STA-03_CCMv3)
- Evaluaciones internas del proveedor (STA-04_CCMv3)
- Gobierno de la cadena de suministro (STA-06_CCMv3, STA-07_CCMv3 y STA-08_CCMv3)
- Auditorías de servicios prestados por terceros (STA-09_CCMv3)
- Seguridad física en los entornos del proveedor que gestionen datos del cliente o se usen para la provisión de alguno de los servicios (DCS-01 a DCS-09_CCMv3)
- Requerimientos sobre sistemas de información de proveedores (SA-9_NISTSP80053)
- Credibilidad (SA-13_NISTSP80053)

Anexo C: Objetivos de medición de los KPIs

C.1. Cumplimiento y supervisión.

C.1.1. Perspectiva de TI general.

Los KPIs definidos para el análisis del cumplimiento y buena gestión de la ciberseguridad deben permitir medir, a nivel general, que se tienen en cuenta a todas las partes clave para la organización desde una perspectiva de Cumplimiento y Gobierno. Asimismo, debe medirse el alineamiento entre las funciones encargadas de la protección y supervisión de los recursos de TI y el resto de la organización.

Otro de los aspectos clave a evaluar es la madurez de las estructuras organizativas que dan soporte a las funciones de seguridad corporativa y de auditoría interna, así como la adecuada comunicación entre estos elementos.

C.1.2. Perspectiva cloud.

El aspecto principal a la hora de integrar servicios cloud en esta categoría de mediciones es el nivel de integración del CSP con el resto de las estructuras de gobierno y control, así como con las propias funciones de supervisión y gestión de la ciberseguridad.

Adicionalmente, también debe medirse el grado en el que el proveedor cumple con sus obligaciones, en lo que respecta tanto al servicio adquirido como al resto de obligaciones que se articulan en torno a éste.

C.2. Gestión del riesgo.

C.2.1. Perspectiva TI general.

Este grupo de KPIs deben validar el análisis y gestión continuos del riesgo tecnológico, considerando además en qué medida estas actividades tienen en cuenta la situación actualizada del cliente.

Por otro lado, también es conveniente asegurar que en la elaboración del análisis de riesgo se adopta un alcance suficiente, que permita asegurar no solo que se dispone de información relevante, sino que no se dejan de lado aspectos relevantes que afecten a estas actividades.

C.2.2. Perspectiva cloud.

Las mediciones en esta categoría asegurarán que el servicio cloud, el CSP, y la infraestructura tecnológica de soporte se integran adecuadamente dentro de la gestión global del riesgo tecnológico de la organización. Para ello, es importante validar que estos servicios no se encuentren sobrerrepresentados en el análisis, y que los riesgos asociados al servicio cloud sean tenidos en cuenta siguiendo criterios homogéneos con el resto de los riesgos cubiertos en el análisis.

También es importante validar que el CSP participa y se involucra, en la medida en la que le afecte, en la gestión de riesgos tecnológicos, especialmente cuando estos riesgos son compartidos entre el cliente y el proveedor.

C.3. Privacidad.

C.3.1. Perspectiva TI general.

En general, los KPIs relacionados con la privacidad evalúan aspectos tantos contractuales, como puede ser la cobertura de los acuerdos de confidencialidad; como otros aspectos de gestión de datos personales. En este último caso, es importante tener en cuenta que deben validarse controles a lo largo de todo el ciclo de vida del dato personal, desde su adquisición, hasta su destrucción.

Con la introducción de la GDPR, otro aspecto clave a evaluar es el grado de cumplimiento con el principio de *privacy by design*.

C.3.2. Perspectiva cloud.

Aunque la gestión de la privacidad con proveedores es un aspecto que debe medirse independientemente de si se hace uso de servicios cloud o no, en este caso la interacción del CSP con los datos debe quedar cubierta, y deberá tratar de analizarse el cumplimiento de éste con las restricciones de localización de los datos. Por último, otro aspecto a cubrir mediante KPIs es la diligencia con la que como clientes se supervisa la gestión de la privacidad del CSP.

C.4. Gobierno y protección del dato.

C.4.1. Perspectiva TI general.

En general, este conjunto de KPIs medirá los medios provistos por la organización para asegurar que mantiene el control sobre sus datos y los protege. Por un lado, se analizará si todos los datos están identificados y tienen un responsable. Asimismo, se evaluará la gestión a lo largo de todo el ciclo de vida de los datos, desde su originación o captura, hasta su destrucción.

Además de la gestión de los datos, debe comprobarse que los datos cuentan con la calidad suficiente como para ser útiles a la organización. Este conjunto de KPIs cubrirá aspectos de alto nivel, puesto que la calidad de los datos en detalle quedará cubierta con el proceso de CDA.

C.4.2. Perspectiva cloud.

Si bien no existe una diferencia sustancial en los KPIs requeridos para analizar el entorno cloud con respecto a los definidos para otros tipos de entornos, deben tenerse en cuenta las características de estos entornos para poder llevar a cabo las mediciones de forma efectiva.

Este conjunto de KPIs representa uno de esos casos en los que es preferible modificar la medición el indicador, perdiendo homogeneidad, en favor de una mayor precisión, puesto que podría requerirse un nivel de restricción mayor para cumplir con ciertos requerimientos del negocio. En este caso, deberán tratar de medirse aspectos concretos como el control sobre la localización física de los datos.

C.5. Continuidad.

C.5.1. Perspectiva TI general.

La gestión de la continuidad de negocio es un proceso integral que abarca elementos de tipo estratégico, funcional y técnico. Por ello, la medición de este proceso deberá abarcar estos mismos elementos. Desde la madurez en el diseño y la gestión de la continuidad, hasta la ejecución y resultado de las pruebas de continuidad, pasando por el diseño de dichos planes, los KPIs asociados a este dominio deberán asegurar que se disponen de todas las herramientas para dar soporte en caso de ocurrencia de un incidente de seguridad, y que dichas herramientas funcionan de forma razonable.

C.5.2. Perspectiva cloud.

Aunque, por su elasticidad y fácil despliegue, los entornos cloud sean considerados más resilientes que los entornos tradicionales, este tipo de mediciones enfocadas en el servicio cloud deberán validar que no se pierda ningún servicio esencial soportado por la tecnología cloud, y

que se dispone de medios de contingencia para dar respuesta a las incidencias que afecten al entorno en la nube.

C.6. Gestión del cambio y mantenimiento de sistemas.

C.6.1. Perspectiva TI general.

Este dominio se considera crítico por el impacto posterior que una mala gestión del desarrollo de software puede tener sobre los sistemas de información. En general, todas las mediciones estarán orientadas a validar el cumplimiento con los principios de seguridad dentro del ciclo de vida del desarrollo software, y el cumplimiento con buenas prácticas de codificación y parametrización de sistemas.

C.6.2. Perspectiva cloud.

En este dominio existe una doble perspectiva al medir entornos cloud. En lo que respecta a los procesos dentro del ciclo de vida del desarrollo software, los aspectos a analizar son muy similares a los que deben cubrirse en cualquier otro tipo de entorno, y en general no es necesario introducir mejoras sustanciales.

Sin embargo, en caso de que el desarrollo esté delegado en un tercero, deberá adoptarse un enfoque de evaluación que permitan validar la madurez en el gobierno del proceso de desarrollo externalizado.

C.7. Gestión operativa.

C.7.1. Perspectiva TI general.

El objetivo básico de este grupo de mediciones es asegurar que todos los procesos asociados a la gestión y operación de los entornos tecnológicos están documentados y se consideran adecuadas. Asimismo, deberá evaluarse la medida en la que dichos procesos se han diseñado y se operan de forma segura.

C.7.2. Perspectiva cloud.

Estos KPIs no requieren una adaptación específica al entorno cloud. Sí deberá analizarse en qué medida la gestión de los entornos se encuentra centralizada, si bien este aspecto no aplica exclusivamente sobre entornos cloud.

C.8. Interoperabilidad y Portabilidad.

C.8.1. Perspectiva TI general.

Para afrontar con garantías cualquier proceso de cambio de proveedor o de migración entre en-

tornos, deberá comprobarse que la organización cuenta con los medios suficientes para ello, y que los entornos tecnológicos que se usen en cada momento cuenten con unas características básicas de estandarización que hagan posible dicha migración.

C.8.2. Perspectiva cloud.

Desde un punto de vista cloud, estos KPIs medirán, junto con las mediciones generales, el nivel de colaboración del CSP en durante las labores de migración, en caso de que llegara a producirse.

C.9. Gobierno de ciberseguridad.

C.9.1. Perspectiva TI general.

Lo que este conjunto de KPIs se ocupar de medir y analizar es el punto de contacto estratégico entre la organización y la supervisión y la gestión de los riesgos de IT. Este conjunto de KPIs ofrecerá información relevante sobre la medida en la que la gestión del riesgo IT está alineada con los requerimientos de la organización, y si existe un alineamiento entre los objetivos de ciberseguridad y los objetivos corporativos. Asimismo, también permitirán validar si estos procesos cuentan con los recursos y la implicación necesaria para que se satisfagan los objetivos definidos.

C.9.2. Perspectiva cloud.

Si bien el gobierno de la ciberseguridad debería ser único dentro de la organización, sí es necesario analizar en qué medida éste se adapta a las necesidades concretas de los servicios cloud adquiridos, especialmente en lo relativo al uso de los recursos tecnológicos, las responsabilidades de los usuarios, y el cumplimiento de la Política de Seguridad; así como la coordinación entre la organización y el CSP.

C.10. Control de acceso.

C.10.1. Perspectiva TI general.

Este dominio es uno de los más relevantes a la hora de salvaguardar la información y los recursos tecnológicos. Los KPIs definidos dentro de este dominio validarán que los accesos que se produzcan respetan los principios de segregación de funciones, necesidad de saber y mínimos privilegios, y que evolucionan a medida que lo hace el negocio y sus necesidades.

C.10.2. Perspectiva cloud.

A la hora de adaptar este tipo de KPIs a los entornos en la nube, debe tenerse en cuenta el mayor nivel de exposición de éstos en Internet, así como la posible pérdida de control para la gestión de accesos e identidades. Por tanto, los KPIs, si bien persiguen el mismo objetivo que en otro tipo de entornos TI, podrían requerir un cambio en la medición a causa de la restricción en el acceso a la información de control sobre el servicio.

C.11. Protección de la infraestructura tecnológica.

C.11.1. Perspectiva TI general.

Los KPIs dentro de este dominio deben medir y analizar el funcionamiento de todas las y medidas de protección definidas a lo largo de todas las capas de la infraestructura tecnológica.

C.11.2. Perspectiva cloud.

Desde un punto de vista tecnológico, uno de los principales cambios introducidos por los entornos cloud es el uso de la capa del hipervisor. Por tanto, los KPIs definidos dentro de este dominio deberán analizar la adecuada protección del hipervisor. Asimismo, también deberá analizarse el nivel de protección de la información almacenada en entornos compartidos (multi-tenant).

C.12. Monitorización y análisis de sistemas.

C.12.1. Perspectiva TI general.

Estos KPIs analizarán que la monitorización de sistemas cubra aquellos recursos que puedan verse afectados por incidentes de seguridad o mediante los cuales pueda comprometerse información sensible de la organización. Adicionalmente, también validarán que la supervisión sea efectiva, de forma que el proceso de monitorización ofrezca resultados de valor para la organización.

C.12.2. Perspectiva cloud.

Desde un punto de vista cloud, no hay una diferencia sustancial relativa a este dominio de KPIs. En este caso, se pierde cierta capacidad de monitorización, especialmente en el caso de análisis de tipo más técnico, como las pruebas de intrusión, por lo que será necesario incrementar el nivel de abstracción para analizar en qué medida el servicio cloud y el entorno tecnológico que le da soporte son monitorizados adecuadamente.

C.13. Cifrado.

C.13.1. Perspectiva TI general.

Estos KPIs analizarán la efectividad de los medios criptográficos para proteger información sensible de la organización y la adecuada gestión de las claves de cifrado.

C.13.2. Perspectiva cloud.

No hay diferencias para este dominio de KPIs con respecto a otros entornos tecnológicos para

entornos de tipo IaaS, si bien la gestión de la criptografía en entornos PaaS y SaaS estará delegada en el proveedor, y por tanto no siempre se podrán analizar estos KPIs en el entorno en la nube.

C.14. Gestión de incidentes de seguridad.

C.14.1. Perspectiva TI general.

La gestión de incidentes de seguridad requiere un conjunto de elementos de tipo estratégico, operativo y técnico que deben funcionar de forma rápida y coordinara para garantizar una adecuada gestión de dichos incidentes. Los KPIs dentro de este dominio evaluaran la eficacia de los medios organizativos y técnicos para identificar, analizar y responder a los incidentes de seguridad. Asimismo, validará aspectos accesorios que facilitan dicha gestión, como el entrenamiento del personal encargado de ofrecer la respuesta, o el cumplimiento de los requerimientos legales que deben tenerse en cuenta para ello.

C.14.2. Perspectiva cloud.

La gestión de incidentes de seguridad de forma coordinada con un proveedor introduce una enorme complejidad en el proceso. Por tanto, estos KPIs analizarán los medios dispuestos para facilitar dicha coordinación, y la eficacia a la hora de ofrecer una respuesta coordinada.

C.15. Gestión de la cadena de valor extendida.

C.15.1. Perspectiva TI general.

Estos KPIs medirán la gestión, tanto desde un punto de vista operativo como de seguridad, de los proveedores de la organización, y de los recursos tecnológicos y organizativos necesarios para ello. En general, este tipo de KPIs se centran en la interacción tecnológica entre dos organizaciones, y en el acceso de terceros a los recursos propios.

C.15.2. Perspectiva cloud.

A diferencia de otro tipo de entornos, estos KPIs también mide la gestión operativa y de la seguridad del recurso externo, aunque en este caso es la propia organización la que accede a recursos tecnológicos externos.

Anexo D: Definición de un mapa de riesgos tecnológicos cloud

Considerando una visión del riesgo expresada como la materialización de una determinada amenaza sobre un activo, en este anexo se desarrolla un mapa de riesgos tecnológicos asociados a entornos cloud. Dicho mapa de riesgos se deberá integrar con el mapa de riesgos tecnológicos general utilizado por la organización, y establecerse mapeos entre los riesgos contenidos en ambos mapas.

Para la definición del mapa de riesgos deben tenerse en cuenta dos elementos básicos. En primer lugar, las amenazas a las que estén sujetas los servicios cloud. En segundo lugar, los controles aplicados sobre los recursos cloud, que reducirán el riesgo asociado a la materialización de dichas amenazas.

D.1. Amenazas cloud.

A continuación, se expone un listado de las principales amenazas con impacto en los servicios cloud:

- Fugas de información
- Deficiencias en los procesos de identificación y gestión de accesos
- Vulnerabilidades presentes en APIs en interfaces
- Secuestro de cuentas o servicios
- Usuarios maliciosos
- Pérdida de información
- Falta de due diligence
- Abuso o uso indebido de servicios cloud
- APTs
- Denegación de servicio
- Falta de capacidad de detección de incidencias
- Phishing
- Falta de gobierno del servicio
- Inadecuada gestión del riesgo tecnológico

D.2. Amenazas asociadas a controles CCM.

A partir de estas amenazas, se analizará a cuál de ellas dan respuesta los controles definidos en la matriz de controles cloud (CCM), por ser un marco de control de referencia especialmente diseñado para la protección de servicios en la nube y ampliamente aceptado por la industria.

El primer paso, consiste en identificar el riesgo y amenaza asociada a cada control:

- **Cumplimiento y aseguramiento**
  - (AAC-1) Materialización de riesgos sobre el servicio cloud que pasen desapercibi dos por parte del cliente como resultado de una supervisión deficiente o ausencia de la misma, lo que provoque un incremento en los costes derivados de su materialización y posterior gestión.
  - (AAC-1) Pérdidas económicas para la organización asociadas a la operación de procesos que utilicen datos incorrectos o inexactos, como resultado de una falta de supervisión de éstos por parte del cliente, cuando se encuentran almacenados en la nube o son transferidos a/desde ésta.
  - (AAC-2) Ineficiencia en la gestión o pérdida de control sobre los riesgos identificados con impacto en el servicio cloud o en los SI/TI corporativos a causa de una falta de seguimiento de dichos riesgos.
  - (AAC-3) Incumplimiento de requerimientos legales u otro tipo de requerimiento externo a la organización y exigible a ésta por una falta de identificación de dichos requerimientos o consideración de los mismos durante la definición de controles que salvaguarden los SI/TI o los servicios cloud adquiridos.
- **Gobierno y gestión del riesgo**
  - (GRM-01) Vulneración del servicio o de los recursos tecnológicos con los que éstos interactúan por una falta de controles implantados sobre éstos, productos de una incorrecta identificación del riesgo asociados a estos elementos y de sus requerimientos mínimos de seguridad.
  - (GRM-02) Protección inadecuada del servicio o los recursos con los que éstos interactúa, o desaprovechamiento de recursos, por una incorrecta identificación de los recursos en los que se almacena información, como resultado de falta de gobierno del dato.
  - (GRM-03 y GRM-05) Uso inadecuado del servicio, pérdida o fuga de información, o debilitación de la protección de los recursos tecnológicos frente a un ciberataque, como resultado de una falta de soporte del gobierno de la ciberseguridad por parte de la alta dirección y la gerencia.
  - (GRM-04) Uso ineficiente de recursos por una falta de alineamiento con los requerimientos del negocio con respecto al servicio, resultado de la ausencia de un programa de seguridad que alinee el gobierno de la ciberseguridad con el negocio.
  - (GRM-06 y GRM-09) Uso ineficiente de recursos por una falta de alineamiento entre

los requerimientos del negocio y la gestión del servicio cloud, como resultado de una ausencia o falta de actualización de políticas, procedimientos y estándares que regulen la operación y gestión del servicio.

- (GRM-07 y HRS-09) Uso indebido del servicio por una ausencia de procedimientos que establezca las normas de uso aceptable y las acciones previstas en caso de incumplimiento.
- (GRM-08 y GRM-10) Uso ineficiente de recursos e incremento de la exposición frente a amenazas por una falta de alineamiento entre los riesgos a los que la organización se vé expuesta en cada momento, y que quedan incorrectamente reflejados en el análisis de riesgo, y los controles definidos para mitigar dichos riesgos.
- (GRM-11 y GRM-12) Uso ineficiente de recursos e incremento en la exposición frente a amenazas por la ausencia de un sistema de gestión de riesgos que analice y disminuya los niveles de riesgo hasta un punto aceptable formalmente aprobado por la organización.

• **Seguridad de aplicaciones e interfaces**

- (AIS-01) Explotación de vulnerabilidades técnicas de seguridad en las aplicaciones desplegadas por el CSP para prestar los servicios en la nube contratados.
- (AIS-01) Explotación de vulnerabilidades técnicas de seguridad en aquellos componentes del software desarrollado por la organización que se despliegan en la nube o que interactúan con recursos que se encuentran desplegados en la nube.
- (AIS-01) Aprovechamiento de APIs o cualquier otra tipología de interface utilizada por la organización para comunicarse con los recursos desplegados en la nube o con el propio servicio cloud para acceder a información confidencial o funcionalidades restringidas.
- (AIS-02) Acceso indebido o no autorizado por parte de personal ajeno a la organización a los sistemas internos o a los servicios cloud contratados.
- (AIS-02) Incumplimiento de requerimientos legales por parte de la organización asociados a la falta de análisis y control de los accesos de terceros al servicio cloud o a recursos internos utilizando a éste como pasarela.
- (AIS-02) Incumplimiento de requerimientos de seguridad (internos o externos) por parte de la organización a causa de la falta de control sobre los accesos de terceros al servicio cloud o a través de éste.
- (AIS-03) Pérdida de integridad de datos a causa de falta de control en el proceso de transferencia de información entre los sistemas de la organización y los servicios cloud adquiridos.
- (AIS-03) Pérdida de integridad de los datos gestionados por el servicio en la nube a causa de una falta de control sobre éste.
- (AIS-04) Uso indebido o no autorizado de sistemas de información o servicios cloud a causa de una ausencia de controles suficientes de seguridad o de una falta de alineamiento de éstos con los requerimientos internos y externos de la organización.
- (AIS-04) Desaprovechamiento de recursos como resultado de una falta de alinea-

miento entre los requerimientos de la organización y el uso de los SI/TI, incluyendo sistemas cloud, por falta de un cuerpo documental que traslade los objetivos del negocio a la gestión de los SI/TI.

- **Gestión de la continuidad del negocio**
  - (BCR-01) Indisponibilidad de los SI/TI de la organización por una falta de alineamiento entre la planificación
  - (BCR-02) Ineficacia de los planes de recuperación de contingencias e incidencias de seguridad por una falta de prueba de los mismos, lo que conlleva el incumplimiento de los RTOs y RPOs definidos, y una indisponibilidad no tolerable del servicio cloud, o de aquellos servicios de la organización que se soporten en éste.
  - (BCR-03) Indisponibilidad del servicio cloud por una incorrecta gestión de los medios de respaldo tanto propios como de terceros (CSP) que deban suplir a la infraestructura tecnológica primaria cuando ésta sufra una contingencia que impacte en su disponibilidad.
  - (BCR-04) Indisponibilidad del servicio cloud, o de alguno de los servicios de la organización soportado por éste, a causa de una incorrecta gestión de la configuración, instalación o despliegue del servicio cloud como consecuencia de falta de soporte documental para la ejecución de estas actividades.
  - (BCR-05, BCR-06) No se incluye riesgo asociado por ser de tipo físico sin posibilidad de gestión directa por parte del cliente.
  - (BCR-07) Indisponibilidad del servicio por falta de mantenimiento sobre los componentes software subyacentes controlados por el cliente.
  - (BCR-07) Indisponibilidad del servicio por falta de mantenimiento sobre los componentes hardware/software subyacentes controlados por el CSP.
  - (BCR-08) Indisponibilidad del servicio cloud por falta de medidas de redundancia
  - (BCR-08) Indisponibilidad de servicios soportados por el servicio cloud por falta de medios de redundancia desplegados por el cliente como contingencia frente a una indisponibilidad del servicio cloud.
  - (BCR-09) Incorrecta gestión de un evento adverso que afecte al servicio cloud o cuyo vector de entrada sea dicho servicio, por una falta o deficiencia en la evaluación del impacto del evento en la organización.
  - (BCR-10) Incorrecta gestión de un evento con impacto en la continuidad del servicio en la nube o en el resto de los servicios o sistemas de la organización como resultado de la interrupción del primero por una falta de políticas, procedimientos o controles que establezcan las medidas a adoptar para gestionar las interrupciones de servicio.
  - (BCR-11) Pérdida de aporte de valor del servicio cloud a la organización por una falta de alineamiento entre las necesidades del negocio y la operación o gestión del servicio y los elementos de SI/TI en los que éste se soporta o a los que éste da soporte.
  - (BCR-12) Impacto operativo o económico provocado por la descontinuación o inte-

rrupción del servicio cloud contratado, o por la pérdida de datos almacenados en éste, a causa de una inadecuada política de retención de recursos.

- **Control de cambios y gestión de la configuración**
  - (CCC-01) Selección y adquisición de servicios cloud que no aportar el valor esperado a la organización, o que no soportan las necesidades del negocio, por una falta de procedimientos y controles que aseguren el alineamiento entre el negocio y el proceso de adquisición o gestión de servicios en la nube.
  - (CCC-02) Impacto operativo o económico derivado de una incorrecta gestión del entorno cloud por parte del personal del CSP, cuando dicha gestión impacta sobre el servicio ofrecido.
  - (CCC-03) Uso de un servicio cloud inseguro como consecuencia de la falta de control y seguimiento sobre la calidad y nivel de seguridad del entorno como resultado de los cambios introducidos sobre éste, tanto por parte del CSP como por el propio cliente.
  - (CCC-04) Uso indebido del servicio cloud mediante la instalación de software malicioso en el entorno como resultado de una falta de restricción y control del despliegue de software en dicho entorno.
  - (CCC-05) Desalineamiento entre los requerimientos del negocio y el aporte de valor del servicio en la nube a causa de un gobierno de TI deficiente que impida la adaptación del servicio a medida que se produzcan cambios en el negocio o los requerimientos de éste.
- **Seguridad del datacenter**
  - (DCS-01) Indisponibilidad del servicio por una incorrecta identificación de recursos tecnológicos de soporte o una inadecuada definición de expectativas de nivel de servicio y requerimientos de disponibilidad para cada uno de ellos.
  - (DCS-02, DCS-07, DCS-08 y DCS-09) Acceso físico no autorizado a los recursos tecnológicos que dan soporte al servicio cloud por una falta de controles de acceso físicos y de monitorización.
  - (DCS-03) Introducción de recursos tecnológicos no autorizados en el entorno de la organización y el servicio usado por ésta por una incorrecta identificación de éstos.
  - (DCS-04 y DCS-05) Pérdida o fuga de información sensible por una incorrecta gestión de los recursos tecnológicos cuando éstos se extraen fuera de las instalaciones del cliente o del CSP, o cuando se procede a su eliminación definitiva.
  - (DCS-06) Pérdida o fuga de información sensible por falta de directrices sobre el uso aceptable y protección de los activos.
- **Seguridad de los datos y gestión del ciclo de vida de la información**
  - (DSI-01, DSI-03, DSI-05) Pérdida de información o divulgación no autorizada de la misma como resultado de una incorrecta clasificación de la información y protección acorde al nivel de clasificación asignado, para aquella información almacenada en el entorno en la nube.
  - (DSI-02) Pérdida de calidad de la información o uso incorrecto de ésta por una falta

de control sobre los flujos de información en los que se vea involucrado el servicio en la nube.

- (DSI-02) Incumplimiento regulatorio provocado por un uso incorrecto de la información como resultado de una incorrecta identificación y gestión de los flujos de información que se produzcan en el servicio en la nube o entre el servicio en la nube y el resto de infraestructura del cliente.
- (DSI-04) Uso incorrecto o indebido de la información alojada o gestionada por el servicio cloud, provocado por la falta de directrices y control sobre el etiquetado y gestión de la información.
- (DSI-06) No se incluye riesgo asociado al no ser específico a los entornos cloud.
- (DSI-07) Uso incorrecto o indebido de la información alojada en el servicio cloud por una falta de asignación de propiedad y responsabilidades sobre éstos.
- (DSI-08) Divulgación no autorizada de información por una incorrecta gestión del proceso de eliminación segura de información o destrucción/desechado de medios de almacenamiento asociados.

• **Gestión de claves de cifrado**

- (EKM-01) Suplantación de identidad de un usuario o un recurso tecnológico frente al servicio, o frente a los recursos internos del cliente suplantando el servicio o uno de sus componentes, por una inadecuada gestión de claves o por falta de identificación de su propietario legítimo.
- (EKM-02 y EKM-04) Uso indebido de una cuenta de usuario legítima o del propio servicio por un tercero no autorizado a causa de una incorrecta gestión de claves criptográficas a lo largo de su ciclo de vida.
- (EKM-03) Acceso no autorizado a información sensible a través de las redes de comunicaciones por una incorrecta protección y cifrado de los datos sensibles y las comunicaciones.

• **Seguridad de los recursos humanos**

- En general, no tiene en cuenta aspectos del servicio, dado que se centra en la seguridad de la información en lo que respecta a la interacción de los empleados con la organización
- (HRS-08) Daños provocados sobre la integridad, confidencialidad o disponibilidad del servicio y la información contenida en éste, por una falta de roles y responsabilidades formalmente definidos y comunicaciones a cada uno de los empleados o proveedores que accedan o interactúen con el servicio.

• **Gestión de identidades y accesos**

- (IAM-01) Uso indebido o divulgación de la información de administración o supervisión del servicio como resultado de una inadecuada segregación de esta información del resto de información operativa del servicio.
- (IAM-02) Acceso no autorizado a los recursos tecnológicos o al servicio cloud por

una incorrecta gestión de credenciales en uno o varios puntos de su ciclo de vida.

- (IAM-03 e IAM-13) Exposición no controlada de información alojada en la nube o fallos en la configuración del servicio a causa de una incorrecta gestión de acceso a las herramientas de diagnóstico, administración y configuración del servicio.
- (IAM-04) Uso indebido o no autorizado del servicio en la nube como consecuencia de la falta de normas y procedimientos relativos a la gestión del acceso a los recursos en la nube.
- (IAM-05 e IAM-09) Comisión de acciones fraudulentas o perjudiciales para la organización como resultado de la pérdida de control o de capacidad de supervisión por una inadecuada segregación de funciones en el proceso de gestión y restricción de accesos.
- (IAM-06) Explotación de vulnerabilidades en las aplicaciones desarrolladas por la organización y desplegadas en la nube por falta de restricción de acceso al código fuente de dichas aplicaciones.
- (IAM-07) Comisión de fraude o de acciones perjudiciales para la organización como resultado de una incorrecta o falta de gestión de acceso de terceros ajenos a la organización a los sistemas que se encuentran desplegados en la nube.
- (IAM-08) Suplantación de identidad de usuarios legítimos por falta de medios para el almacenamiento y acceso seguro a las identidades utilizadas para el acceso a los recursos en la nube.
- (IAM-10 e IAM-11) Ejecución de acciones indebidas como resultado de una inadecuada gestión de los cambios en la organización, que provoquen la acumulación innecesaria o no permitida de permisos de acceso de un usuario tras cambiar sus funciones en la organización, o una asignación de permisos desalineada con las funciones desempeñadas.
- (IAM-12) Acceso no autorizado a información sensible de la organización alojada en la nube o uso indebido del servicio por una incorrecta gestión de credenciales.

- **Interoperabilidad y portabilidad**
  - (IPY-01, IPY-04 e IPY-05) Problemas de cambio de proveedor (vendor lock-in), con la posibilidad de tener que decomisionar servicios o funcionalidades, o de realizar inversiones económicas no previstas, a causa del uso de APIs de código propietario, protocolos de red no estandarizados o plataformas de virtualización que hagan uso de formatos no estandarizados que no sean portables a otro proveedor.
  - (IPY-02) Problemas de cambio de proveedor (vendor lock-in), pudiendo incurrir en la pérdida de información relevante para la organización, por la imposibilidad de recuperar aquellos datos no estructurados del cliente alojados en la infraestructura del CSP a los que dicho cliente no tenga acceso directo.
  - (IPY-03) Pérdida de alineamiento entre las necesidades del negocio y el servicio a causa de una incorrecta definición de acuerdos de servicio con el CSP en los que se recojan tanto los requerimientos funcionales del servicio, como los no funcionales.
  - (IPY-04) Incumplimiento regulatorio por parte del cliente a causa de una incorrecta

definición de acuerdos de servicio con el CSP en los que se especifiquen los requerimientos no funcionales del cliente con impacto legal.

- **Seguridad de la infraestructura y virtualización**
  - (IVS-01) Uso indebido o no autorizado de los recursos de información que permanece indetectado por una incorrecta protección de los registros de auditoría a lo largo de todo su ciclo de vida.
  - (IVS-02) Pérdida de integridad o disponibilidad de la información almacenada en el servicio cloud por una incorrecta gestión de cambios en las máquinas virtuales que dan soporte al servicio.
  - (IVS-03) Problemas de comunicación entre sistemas o servicios, o problemas de correlación de eventos, por una mala gestión de las fuentes horarias configuradas en los sistemas utilizados por el cliente.
  - (IVS-04) Imputación de costes no previstos asociados al servicio cloud contratado por una incorrecta gestión y planificación de la capacidad de los sistemas.
  - (IVS-05) Ciberataques que tienen como vector de ataque el servicio cloud, que explotan vulnerabilidades no identificadas por el cliente en la infraestructura controlada por éste (aplica de la misma manera a la infraestructura del proveedor) como resultado del uso de herramientas de detección de vulnerabilidades no adaptadas a las tecnologías cloud.
  - (IVS-06, IVS-10 e IVS-12) Ciberataques que aprovechan una falta de segregación, protección o monitorización del tráfico de red generado para la comunicación entre el servicio cloud y el resto de la infraestructura del cliente, o entre el servicio cloud y el exterior, tanto para labores de operación del servicio, como de administración de éste.
  - (IVS-07) Ciberataques que aprovechan la falta de una configuración robusta de la capa de sistema operativo de la infraestructura cloud para explotar puertos no utilizados o mal configurados, protocolos inseguros, o aprovechar la ausencia de medidas de seguridad dentro del propio sistema operativo.
  - (IVS-08) Falta de control del software en explotación, pudiendo provocar el acceso no autorizado a información sensible o la divulgación no controlada de ésta, por una incorrecta segregación entre entornos de desarrollo y producción, y deficiencias en los procedimientos de promoción de cambios a producción.
  - (IVS-09) Este control está centrado en el CSP, por lo que no se considera para este listado
  - (IVS-11) Uso indebido o no autorizado del servicio cloud, o divulgación no autorizada de la información propiedad del cliente usada por éste, causado por una escalada privilegios aprovechando la falta de segregación o protección de las sesiones y comunicaciones de administración de la infraestructura, y las sesiones y comunicaciones de operación del servicio.
- **Seguridad móvil**
  - Este dominio no tiene un impacto específico en el servicio cloud, por lo que no se

incorpora en este análisis, al entenderse que es independiente del modelo de arquitectura tecnológica usado por la organización.

- **Gestión de incidencias**
  - (SEF-01) Incumplimientos legales por fallos de comunicación con las autoridades legislativas o de control en caso de que se produzca un incidente de seguridad que afecte al servicio cloud y que requiera de una investigación forense posterior.
  - (SEF-02 y SEF-05) Pérdida de disponibilidad de funciones críticas para el negocio soportadas por el servicio cloud, o pérdida de integridad o confidencialidad de la información usada por el servicio, causada por deficiencias en los procedimientos de gestión de incidentes de seguridad definidos por el cliente.
  - (SEF-03 y STA-02) Fallos en la gestión de incidentes de seguridad, con impacto en la integridad, confidencialidad o disponibilidad de la información usada por el servicio cloud, causados por deficiencias en la comunicación entre el cliente y actores externos con los que éste se relacione (principalmente proveedores).
  - (SEF-04) Pérdidas económicas desproporcionadas o no justificadas, resultantes de una resolución judicial desfavorable para la organización, cuando ésta tuviera como base una investigación forense realizada sobre el servicio cloud, por el desalineamiento entre el proceso de investigación forense seguido y los requerimientos legales para que dicho proceso se considere válido.
- **Gestión de la cadena de suministro, transparencia y responsabilidad**
  - (STA-01) Pérdida de calidad de la información gestionada por el servicio cloud como resultado de una falta de validación de dicha calidad en el momento en el que la información es obtenida de un tercero.
  - (STA-03) Pérdida de disponibilidad del servicio cloud por una falta de proyección de requerimientos de nivel de servicio y capacidad durante las fases de diseño y desarrollo de la tecnología en la que se sustenta en servicio.
  - (STA-04) Desalineamiento prolongado con los requerimientos del negocio y otros requerimientos no funcionales (seguridad y cumplimiento principalmente), por falta de revisión de la adecuación de los proveedores a dichos requerimientos
  - (STA-05) Desalineamiento entre las necesidades del cliente y las características del servicio cloud contratado o su gestión por parte del CSP provocado por la ausencia de acuerdos de provisión de servicio completos y suficientemente detallados.
  - (STA-06 y STA-08) Desalineamiento entre el negocio y el servicio cloud, o pérdida de integridad, confidencialidad y disponibilidad, causados por la incorrecta gestión de los proveedores de los riesgos TI presentes en sus cadenas de valor extendidas.
  - (STA-07) Desalineamiento entre las necesidades del negocio y las características del servicio cloud por una falta de seguimiento de los acuerdos de servicio y SLAs por parte del cliente.

- (STA-09) Pérdida de visibilidad sobre los riesgos TI introducidos por proveedores externos sobre el servicio cloud como consecuencia de una estrategia de aseguramiento incorrecta o deficiencias en la supervisión de dichos proveedores, independientemente de si esta la realiza el cliente o un tercero independiente.

- **Gestión de vulnerabilidades y amenazas**
  - (TVM-01 y TVM-03) Infecciones por malware o ejecución no autorizada de software como resultado de la falta de políticas, procedimientos y herramientas que protejan frente a este tipo de amenazas.
  - (TVM-02) Acceso indebido o no autorizado a los recursos tecnológicos de la organización aprovechando vulnerabilidades presentes en los sistemas sobre los que no se dispone de un proceso adecuado de identificación de vulnerabilidades técnicas y parcheado.

D.3. Consolidación de amenazas asociadas a controles CCM.

A partir de la identificación previa de riesgos y amenazas, se establecerán categorías más generales de amenazas en las que agrupar los elementos previamente identificados y que puedan mapearse con las principales amenazas a las que se ven expuestos los servicios cloud, recogidas en el primer apartado del presente anexo.

Controles asociados	Riesgo basado en controles	Amenaza asociada
Dominio: cumplimiento y aseguramiento		
AAC-1	Incorrecta identificación y tratamiento de riesgos por parte del cliente por falta de supervisión	Pérdida de visibilidad sobre el riesgo TI / Fallos en la gestión del riesgo TI
AAC-1	Falta de supervisión sobre controles y datos almacenados en la nube	Uso de datos incorrectos
AAC-2	Ineficiencias en la gestión de los riesgos por falta de seguimiento de su tratamiento	Falta de control sobre los riesgos
AAC-3	Incumplimiento de requerimientos regulatorios no trasladados al CSP contractualmente	Incumplimientos regulatorios
Dominio: Gobierno y gestión del riesgo		
GRM-01	Falta de identificación de requerimientos mínimos de seguridad del servicio cloud	Vulneración del servicio
GRM-02	Ausencia de gobierno del dato cuando éste se almacena en la nube	Protección inadecuada del servicio
GRM-03 GRM-05	Falta de recursos para el gobierno de ciberseguridad	Uso inadecuado / indebido del servicio
GRM-04	Desalineamiento entre el gobierno de ciberseguridad y las expectativas del negocio del servicio cloud	Pérdida de aporte de valor para la organización / Desaprovechamiento de recursos
GRM-06 GRM-09	Falta de un cuerpo normativo interno adaptado al uso de servicios cloud	Pérdida de aporte de valor para la organización / Desaprovechamiento de recursos
GRM-07 HRS-09	Ausencia de procedimientos o normas de uso aceptable del servicio cloud	Uso inadecuado / indebido del servicio

GRM-08 GRM-10	Falta de un análisis de riesgos que considere los principales riesgos del servicio cloud para la organización	Pérdida de aporte de valor para la organización / Desaprovechamiento de recursos
GRM-08 GRM-10		Falta de control sobre los riesgos
GRM-11 GRM-12	Ausencia de tratamiento para aquellos riegos que se identifiquen y que afecten al servicio cloud	Pérdida de aporte de valor para la organización / Desaprovechamiento de recursos
Dominio: Seguridad de Aplicaciones e Interfaces		
AIS-01	Uso de APIs no estandarizadas o con vulnerabilidades técnicas no testeadas	Vulneración del servicio
AIS-02	Falta de identificación de requerimientos de seguridad para el acceso al servicio cloud	Uso indebido o no autorizado de recursos
AIS-02		Incumplimientos regulatorios
AIS-03	Pérdida de control o calidad sobre la información durante las migraciones	Uso de datos incorrectos
AIS-04	Incorrecta protección de las interfaces de comunicación con el servicio	Uso inadecuado / indebido del servicio
Dominio: Gestión de la Continuidad del Negocio y Resiliencia Operacional		
BCR-01	Marco de gestión de la continuidad no adaptado al servicio cloud	Indisponibilidad de los SI/TI
BCR-02	Ausencia de pruebas sobre los servicios cloud de los planes de respuesta ante incidentes	Indisponibilidad de los SI/TI
BCR-03	Falta de protección de los recursos tecnológicos y facilities de los que el servicio cloud es dependiente	Indisponibilidad de los SI/TI
BCR-04	Ausencia de documentación sobre la configuración, despliegue y uso del servicio cloud	Indisponibilidad de los SI/TI
BCR-07	Falta de mantenimiento de los componentes asociados al servicio cloud	Indisponibilidad de los SI/TI
BCR-08	Ausencia de redundancias sobre el servicio cuando éste soporte procesos críticos	Indisponibilidad de los SI/TI
BCR-09	Fallos en la estimación de la criticidad del servicio cloud a partir de los procesos críticos soportados y su tolerancia a interrupciones	Indisponibilidad de los SI/TI
BCR-10	Deficiencias en la comunicación de los requerimientos de disponibilidad y continuidad a los proveedores	Indisponibilidad de los SI/TI
BCR-11	Incorrecta asignación de roles y responsabilidades para la gestión de incidencias y la continuidad	Incorrecta gestión de incidentes
BCR-12	Fallos en la recuperación de información contenida en el servicio durante el proceso de restauración tras un incidente	Pérdida / Fugas de información
Dominio: Control de Cambios y Gestión de la Configuración		
CCC-01	Ausencia de roles de supervisión y control del servicio cloud	Pérdida de aporte de valor para la organización / Desaprovechamiento de recursos

CCC-02	Inadecuado control de los empleados de proveedores y protección de los recursos a los que éstos accedan	Incorrecta gestión de recursos externalizados
CCC-03	Falta de supervisión técnica u operativa de la calidad del servicio	Pérdida de calidad del servicio
CCC-04	Ausencia de procedimientos y controles que prevengan la instalación no autorizada de software	Instalación de software malicioso
CCC-05	Introducción de cambios no controlados en el servicio cloud, incluyendo falta de trazabilidad o validación de éstos	Falta de gobierno del servicio
Dominio: Seguridad del Centro de Datos		
DCS-01	Ausencia de identificación de las características de los servicios cloud contratados, y de requerimientos operativos y de seguridad de los mismos	Indisponibilidad de los SI/TI
DCS-02 DCS-07 DCS-08 DCS-09	Ausencia de controles físicos de acceso a los recursos tecnológicos que soportan el servicio cloud	Acceso físico no autorizado
DCS-03	Suplantación de identidad falsificando la identidad de un dispositivo legítimo	Uso de recursos maliciosos / no autorizados
DCS-04 DCS-05	Falta de control del acceso y uso del servicio cloud fuera de las instalaciones de la organización	Pérdida / Fugas de información
DCS-06	Ausencia de directrices sobre el uso seguro del servicio cloud	Pérdida / Fugas de información
Dominio: Seguridad de los Datos y Gestión del Ciclo de Vida de la Información		
DSI-01	La información utilizada y almacenada en el servicio cloud no se encuentra correctamente clasificada según su criticidad para el negocio	Pérdida / Fugas de información
DSI-02	Falta de identificación, protección y mantenimiento de los datos y flujos de información utilizados por el servicio cloud	Uso de datos incorrectos
		Pérdida / Fugas de información
DSI-03	Los datos que viajan por redes públicas no se encuentran debidamente protegidos	Pérdida / Fugas de información
		Fraude
		Uso de datos incorrectos
DSI-04 DSI-05 DSI-06	No se han definido requerimientos para el etiquetado, protección y manipulación de los datos almacenados o gestionados por el servicio cloud	Uso indebido o no autorizado de recursos
		Pérdida / Fugas de información
DSI-07	Los datos usados por el servicio no disponen de un responsable asignado, ni se ha identificado el uso que hace el servicio de éstos	Uso indebido o no autorizado de recursos
		Pérdida / Fugas de información
DSI-08	Falta de medidas de seguridad para garantizar la destrucción / eliminación de la información confidencial	Pérdida / Fugas de información
Dominio: Gestión de Claves de Cifrado		
EKM-01	Incorrecta gestión de las asignaciones de claves criptográficas a la identidad de cada usuario	Suplantación de identidad de un usuario o un servicio
EKM-02	Gestión no controlada o insegura de claves de cifrado a lo largo de todo su ciclo de vida	Uso inadecuado / indebido del servicio
		Suplantación de identidad de un usuario o un servicio
EKM-03	Falta de control de los protocolos de cifrado utilizados para la protección de datos sensibles	Uso indebido o no autorizado de recursos

EKM-04	Uso de protocolos de cifrado no estandarizados ni validados para asegurar su robustez	Vulneración del servicio
Dominio: Recursos Humanos		
HRS-08	Incorrecta asignación y gestión de roles y responsabilidades para la gestión del servicio y la información contenida en éste	Daños provocados por usuarios maliciosos
Dominio: Gestión de Identidades y Accesos		
IAM-01	Acceso no autorizado a las herramientas de auditoría del servicio cloud	Pérdida / Fugas de información
		Uso inadecuado / indebido del servicio
IAM-02 IAM-12	Incorrecta gestión del ciclo de vida de las identidades utilizadas por los usuarios o de los permisos de acceso de éstos	Uso indebido o no autorizado de recursos
IAM-03 IAM-13	Acceso no autorizado a puertos de diagnóstico o configuración, o a programas que anulen parcial o totalmente las medidas de seguridad desplegadas	Pérdida / Fugas de información
		Fallos en la configuración
IAM-04	Falta de identificación de los requerimientos para la gestión de identidades y perfilado de usuarios	Uso inadecuado / indebido del servicio
IAM-05 IAM-09	Incorrecta restricción de acceso de los distintos perfiles de usuario al servicio cloud, impidiendo la segregación de funciones para el acceso y gestión del servicio.	Fraude
IAM-06	Los aplicativos/sistemas desplegados en el servicio no permiten la aplicación del principio de menor privilegios	Uso indebido o no autorizado de recursos
		Fraude
IAM-07	No se disponen de medidas que garanticen la restricción y supervisión de los accesos al servicio cloud realizado por personal externo	Fraude
		Uso indebido o no autorizado de recursos
IAM-08	No existe una adecuada restricción de acceso a las identidades utilizadas para la autenticación en el servicio cloud	Suplantación de identidad de un usuario o un servicio
IAM-10	Falta de autorización y revisión de los accesos realizados al servicio cloud y de los permisos asignados a los usuarios	Uso inadecuado / indebido del servicio
IAM-11	Falta de control en la revocación de accesos de los usuarios del cliente o del CSP al servicio cloud o su infraestructura tecnológica de soporte	Uso inadecuado / indebido del servicio
Dominio: Interoperabilidad y Portabilidad		
IPY-01	Uso de APIs no estandarizadas o de código abierto	Vendor Lock-in
IPY-02	Falta de acceso o de funcionalidades de descarga masiva de los datos almacenados en la nube	Vendor Lock-in

IPY-03	Ausencia de requerimientos funcionales y no funcionalidades trasladados al CSP para la comunicación automatizada de información	Pérdida de aporte de valor para la organización / Desaprovechamiento de recursos
IPY-04	Uso de protocolos de red no estandarizados o inseguros	Pérdida / Fugas de información
		Uso inadecuado / indebido del servicio
IPY-05	Uso de una plataforma de virtualización incompatible con formatos de virtualización estandarizados	Vendor Lock-in
Dominio: Seguridad de la Infraestructura y Virtualización		
IVS-01	Protección inadecuada de los registros de auditoría	Incumplimientos regulatorios
		Uso de datos incorrectos
IVS-02	Falta de integridad en las imágenes de las máquinas virtuales o sus variables de estado	Uso de datos incorrectos
IVS-03	Uso de diversas fuentes horarias, o una fuente horaria no fiable, para sincronizar los distintos sistemas de la organización, incluido el servicio cloud	Fallos en la comunicación
IVS-04	Falta de definición de los requerimientos de rendimiento del servicio	Incremento no controlado de consumo de recursos
IVS-05	Uso de herramientas de detección de vulnerabilidades técnicas no adaptadas a las tecnologías cloud	Ciberataques / APTs
IVS-06 IVS-10 IVS-12	El tráfico en los entornos de red virtuales no se encuentra adecuadamente protegido, segregado y monitorizado	Ciberataques / APTs
IVS-07	Los sistemas operativos virtualizados no se someten a un proceso de bastionado	Ciberataques / APTs
IVS-08	No existe segregación entre los entornos productivos y no productivos	Uso indebido o no autorizado de recursos
IVS-11	No se restringe adecuadamente el acceso a las funcionalidades de administración del hipervisor u otras utilidades de gestión de máquinas virtuales	Uso inadecuado / indebido del servicio
Dominio: Gestión de incidentes de seguridad		
SEF-01	No se han identificado los puntos de contacto externos en caso de incidente ni los requerimientos para la comunicación con éstos	Incumplimientos regulatorios
SEF-02	No existen requerimientos ni controles para la identificación, evaluación y clasificación de eventos de seguridad	Indisponibilidad de los SI/TI
SEF-03 STA-02	No se han definido o comunicado las responsabilidades de los empleados para la comunicación y gestión de incidentes de seguridad	Incorrecta gestión de incidentes
SEF-04	No se han identificado o tenido en cuenta los requerimientos regulatorios o contractuales asociados a la gestión de incidentes	Incumplimientos regulatorios

SEF-05	No se evalúa la capacidad de respuesta a incidentes	Indisponibilidad de los SI/TI
Dominio: Gestión de la cadena de suministro, Transparencia y Responsabilidad		
STA-01	No se exige a los proveedores la definición de controles que garanticen que la calidad de los datos se mantiene cuando éstos son gestionados por dichos proveedores	Uso de datos incorrectos
STA-02	No se han establecido contractualmente los requerimientos del proveedor para la gestión de incidentes	Uso de datos incorrectos
STA-03	No se tiene en cuenta los requerimientos de disponibilidad y nivel de servicio durante el diseño de recursos tecnológicos desplegados en cloud o sobre los que el servicio se soporte	Indisponibilidad de los SI/TI
STA-04	No se exige a los proveedores la realización de evaluaciones de cumplimiento y efectividad de sus controles para la gestión del riesgo TI	Pérdida de aporte de valor para la organización / Desaprovechamiento de recursos
STA-05	No se trasladan a los proveedores acuerdos de cadena de suministro suficientemente detallados como para asegurar la satisfacción de las necesidades del negocio	Pérdida de aporte de valor para la organización / Desaprovechamiento de recursos
STA-06	Los proveedores no validan la gestión del riesgo y gobierno de TI de las organizaciones de las que éstos dependen para la provisión del servicio al cliente	Uso de datos incorrectos
STA-07	El cliente no ha definido controles que garanticen el cumplimiento de los SLAs, y que permitan la corrección de desviaciones	Pérdida de aporte de valor para la organización / Desaprovechamiento de recursos
STA-08	El cliente no exige al proveedor la aplicación de controles para salvaguardar la seguridad de la información a lo largo de las cadenas de suministro de éstos	Pérdida de aporte de valor para la organización / Desaprovechamiento de recursos Uso de datos incorrectos
STA-09	No se exigen evidencias a los proveedores de la evaluación del cumplimiento con los requerimientos funcionales y no funcionales exigidos por el cliente	Pérdida de visibilidad sobre el riesgo TI / Fallos en la gestión del riesgo TI
Dominio: Gestión de vulnerabilidades y amenazas		
TVM-01	No existen controles que impidan la ejecución de malware	Instalación de software malicioso
TVM-02	No se controla la gestión y despliegue de parches de seguridad y actualizaciones sobre los recursos tecnológicos	Uso indebido o no autorizado de recursos
TVM-03	No existen controles que impidan la ejecución de código móvil no autorizado	Instalación de software malicioso

D.4. Mapeo entre amenazas generalistas y amenazas asociadas a controles.

Para asegurar que las amenazas identificadas en la tabla previa cubran aquellas con mayor impacto sobre los servicios cloud identificadas al inicio del presente anexo, en la siguiente tabla se establece una matriz de mapeo en la que puede comprobarse que no solo se han identificado todas las amenazas cubiertas por los controles de la matriz CCM, sino que además éstas cubren aquellas amenazas generalmente asociadas a los servicios en la nube:

Incumplimientos regulatorios	Falta de control sobre los riesgos	Uso de datos incorrectos	Pérdida de visibilidad sobre el riesgo TI / Fallos en la gestión del riesgo TI	
				Fugas de información
				Deficiencias en los procesos de identificación y gestión de accesos
				Vulnerabilidades presentes en APIs en interfaces
				Secuestro de cuentas o servicios
				Usuarios maliciosos
		X		Pérdida de información
X	X		X	Falta de due diligence
				Abuso o uso indebido de servicios cloud
				APTs
				Denegación de servicio
			X	Falta de capacidad de detección de incidencias
				Phishing
X	X		X	Falta de gobierno del servicio
X	X		X	Inadecuada gestión del riesgo tecnológico

Incorrecta gestión de recursos externalizados	Incorrecta gestión de incidentes	Indisponibilidad de los SI/TI	Uso inadecuado / indebido del servicio	Protección inadecuada del servicio	Vulneración del servicio	
					X	Fugas de información
				X		Deficiencias en los procesos de identificación y gestión de accesos
				X	X	Vulnerabilidades presentes en APIs en interfaces
					X	Secuestro de cuentas o servicios
			X		X	Usuarios maliciosos
						Pérdida de información
						Falta de due diligence
			X		X	Abuso o uso indebido de servicios cloud
		X			X	APTs
		X			X	Denegación de servicio
	X	X				Falta de capacidad de detección de incidencias
			X			Phishing
X				X		Falta de gobierno del servicio
X	X			X		Inadecuada gestión del riesgo tecnológico

Pérdida / Fugas de información	Uso de recursos maliciosos / no autorizados	Acceso físico no autorizado	Falta de gobierno del servicio	Instalación de software malicioso	Pérdida de calidad del servicio	
X						Fugas de información
		X				Deficiencias en los procesos de identificación y gestión de accesos
	X					Vulnerabilidades presentes en APIs en interfaces
						Secuestro de cuentas o servicios
	X			X		Usuarios maliciosos
X						Pérdida de información
						Falta de due diligence
	X					Abuso o uso indebido de servicios cloud
	X			X		APTs
					X	Denegación de servicio
						Falta de capacidad de detección de incidencias
X						Phishing
			X		X	Falta de gobierno del servicio
			X	X		Inadecuada gestión del riesgo tecnológico

Pérdida de aporte de valor para la organización / Desaprovechamiento de recursos	Vendor Lock-in	Fallos en la configuración	Daños provocados por usuarios maliciosos	Suplantación de identidad de un usuario o un servicio	Fraude	
X						Fugas de información
				X		Deficiencias en los procesos de identificación y gestión de accesos
		X				Vulnerabilidades presentes en APIs en interfaces
				X		Secuestro de cuentas o servicios
			X		X	Usuarios maliciosos
						Pérdida de información
						Falta de due diligence
					X	Abuso o uso indebido de servicios cloud
					X	APTs
						Denegación de servicio
						Falta de capacidad de detección de incidencias
X	X				X	Phishing
	X					Falta de gobierno del servicio

Ciberataques / APTs	Incremento no controlado de consumo de recursos	Fallos en la comunicación	Uso indebido o no autorizado de recursos	
				Fugas de información
			X	Deficiencias en los procesos de identificación y gestión de accesos
				Vulnerabilidades presentes en APIs en interfaces
			X	Secuestro de cuentas o servicios
			X	Usuarios maliciosos
				Pérdida de información
				Falta de due diligence
X			X	Abuso o uso indebido de servicios cloud
X				APTs
		X		Denegación de servicio
				Falta de capacidad de detección de incidencias
				Phishing
	X			Falta de gobierno del servicio
			X	Inadecuada gestión del riesgo tecnológico

Referencias

- Alawadhi, A; et al. (2015). Audit Analytics and Continuous Audit. Looking Toward the Future. American Institute of Certified Public Accountants.
- Sabau, A; et al. (2011). Fundamentals of continuous auditing and monitoring in enterprise resource planning systems. Mathematics and Computers in Biology, Business and Acoustics. Disponible en: https://www.researchgate.net/publication/228401522
- Coderre, D. (2015). Global Technology Audit Guide. Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment. The Institute of Internal Auditors.
- Whitehouse, T; et al. (n.d.). How Data Analytics and Continuous Auditing and Monitoring Are Evolving. Compliance Week.
- Mello Codesso, M; Lunkes, R. J; da Silva, P. C. (2017). Proposal of Continuous Audit Model. Data Integration Framework. The Twelfth International Conference on Internet and Web Applications and Services.
- Ko R. K. L; et al. (2011). TrustCloud: A Framework for Accountability and Trust in Cloud Computing. 2nd IEEE Cloud Forum for Practitioners.
- (n.d.). (2017). Cybersecurity and Continuous Assurance. Journal of Emerging Technologies in Accounting. Volumen 4. Número 1, p. 1-12.
- Chiu V; et al. (2018). Continuous Auditing: Theory And Application. Rutgers Studies in Accounting Analytics. Emerald Publishing.
- Boob, R. N; Rokade, S. M. (2016). A Review on Continuous Public Auditing Scheme for Regenerating Code Based Secure Cloud Storage. International Journal of Engineering Development and Research. Volumen 4. Número 4.
- (n.d.). (2016). Continuous Monitoring and Compliance in the Cloud. Evident.io.
- (n.d.). (2017). The 2017 State of Cybersecurity Metrics Annual Report. Thycotic.
- Vaulx, F; et al. (2018). NIST Special Publication 500-307. Cloud Computing Service Metrics Description. National Institute of Standards and Technology. Departamento de Comercio de Estados Unidos.
- Mogull, R; et al. (2017). Security Guidance For Critical Areas of Focus In Cloud Computing v4.0. Cloud Security Alliance.
- Marques, R. P; Santos, H; Santos, C. (2013). A conceptual model for evaluating systems with continuous assurance services. International Conference on Health and Social Care Information Systems and Technologies.
- Vasarhelyi, M. A. (n.d.). Continuous audit: today and tomorrow. Continuous Audit and Reporting Laboratory. Rutgers Business School. Newark and New Burnswick.
- Chan, D. Y; Vasarhelyi, M. A. (n.d.). Innovation and Practice of Continuous Auditing. Rutgers

Business School.
- Alles, M. G; Kogan, A; Vasarhelyi, M. A. (2008). Putting Continuous Auditing Theory into Practice: Lessons from Two Pilot Implementation. Journal of Information Systems. Volumen 22. Número 2. P 195-214.
- Moon, D. Continuous Risk Monitoring and Assessment (CRMA): Framework for Risk based CA.
- Hulstijn, J; et al. (n.d.). Continuous Control Monitoring-based Regulation: a case in the meat processing industry. Delft University of Technology, VU University, Thauris B. V. La Haya.
- Warren, J. D; Smith, L. M. (2006). Continuous Auditing: An Effective Tool for Internal Auditors. Working Paper. Disponible en: https://www.researchgate.net/publication/228307292
- Ponz Lillo, D; et al. (2014). Guía para implanter con éxito un modelo de Auditoría Continua. Instituto de Auditores Internos de España.
- Tank K.K. (2011). Continuous Auditing & Continuous Monitoring in a Broader Perspective. The Performance Management Potential of CA & CM. Proyecto de Tesis. University of Twente & KPMG. Países Bajos.
- (n.d.). (n.d.). Cloud Controls Matrix (CCM). Cloud Security Alliance. Disponible en: https://cloudsecurityalliance.org/research/cloud-controls-matrix/
- (n.d.). (2015). ISO/IEC 27002. Código de prácticas para los controles de seguridad de la información. AENOR.
- (n.d.). (2015). ISO/IEC 27017. Código de prácticas para los controles de seguridad de la información basado en ISO/IEC 27002 para servicios cloud. AENOR.
- Vaulx, F; et al. (2018). NIST Special Publication 500-307. Cloud Computing Service Metrics Description. National Institute of Standards and Technology. Departamento de Comercio de Estados Unidos.
- Ross, R; et al. (2013). NIST Special Publication 800-53. Security and Privacy Controls for Federal Informatión Systems and Organizations. Revisión 4. National Institute of Standards and Technology. Departamento de Comercio de Estados Unidos.
- Jansen, W; Grance, T. (2011). NIST Special Publication 800-144. Guidelines on Security and Privacy in Public Cloud Computing. National Institute of Standards and Technology. Departamento de Comercio de Estados Unidos.
- Armour, W. W; et al. (n.d.). NIST Special Publication 500-299. NIST Cloud Computing Security Reference Architecture. Draft. National Institute of Standards and Technology. Departamento de Comercio de Estados Unidos.
- Moran, J. (n.d.). Key Performance Indicators (KPIs) for Security Operations and Incident Response. Identifying Which KPIs Should Be Set, Monitored and Measured. DFLabs.
- Chew, E; Swanson, M; Stine, K; Bartol, N; Brown, A; Robinson, W. (2008). NIST Special Publication 800-55 Revision 1. Performance Measurement Guide for Information Security. National Institute of Standards and Technology. Departamento de Comercio de Estados Unidos.
- Nigrini, M. J; Johnson, A. J. (2008). Using Key Performance Indicators and Risk Measures in

Continuous Monitoring. Journal of Emerging Technologies in Accounting. Volumen 5. p. 65-80.
- Vasarhelyi, M. A; Alles, M; Williams, K. T. (2010). Continuous Assurance for the Now Economy. A Thought Leadership Paper for the Institute of Chartered Accountants in Australia.
- (n.d.). (n.d.). 6 Key Risk Management Metrix for Controlling Cyber Security. Xactium.
- Santander, M. H. (2010). Measuring effectiveness in Information Security Controls. Information Security Reading Room. SANS Institute.
- (n.d.). (2008). Understanding and managing the IT risk landscape. A practitioner's guide. CRO Forum.
- Lainhart, J. W; et al. (2012). COBIT 5. Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Organización. An ISACA Framework. ISACA.
- Adler, M; et al. (2007). COBIT 4.1. Marco de Trabajo. Objetivos de control. Directrices Generales. Modelos de Madurez. IT Governance Institute.
- (n.d.). (n.d.). CIS Controls Measures and Metrics for Version 7. CIS Controls.
- Rose, S; Borchert, O; Mitchell, S; Connelly, S. (n.d.). Draft NIST Special Publication 800-207. Zero Trust Architecture. National Institute of Standards and Technology. Departamento de Comercio de Estados Unidos.
- Deshpande, S. (2016). Continuous Auditing in Cloud. 37 WCARS. Australia.
- Vasarhelyi, M. A; Halper, F. (1991). The Continuous Audit of Online Systems. Auditing: A Journal of Practice & Theory. Allen Press. Disponible en: https://www.researchgate.net/publication/255667612
- (n.d.). (2018). Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. National Institute of Standards and Technology. Departamento de Comercio de Estados Unidos.
- Pipino, L. L; Lee, Y, W; Wang, R. Y. (2002). Data Quality Assessment. Communications of the ACM. Volumen 45. Número 4.
- Jonker, R. A. (2012). Data quality assessment. Compact. International edition.
- Batini, C; Cappiello, C; Francalanci, C; Maurino, A. (2009). Methodologies for Data Quality Assessment and Improvement. ACM Computing Surveys. Volumen 41. Número 3. Artículo 16.
- Azarnik, A; Shayan, J; Alizadeh, M; Karamizadeh, S. (2012). Associated Risks of Cloud Computing for SMEs. Open International Jorunal of Informatics. Volumen 1.
- Mosher, R. (2011). Cloud Computing Risks. Information Systems Security Association Jorunal.
- Agarwal, A; Agarwal, A. (2011). The Security Risks Associated with Cloud Computing. International Journal of Computer Applications in Engineering Sciences. Volumen 1.
- Bisong, A; Rahman, S. S. M. (2011). An overview of the Security Concerns in Enterprise Cloud Computing. International Journal of Network Security & Its Applications (IJNSA). Volumen 3. Número 1.
- Brodkin, J. (2008). Gartner: Seven cloud-computing security risks. Network World.
- Bannerman, P. L. (n.d.). Cloud Computing Adoption Risks: State of Play. University of NSV. Sidney. Australia.

- Wooley, P. S. (2011). Identifying Cloud Computing Security Risks. Capstone Report. Applied Information Management. Universidad de Oregón.
- Sharma, M; Husain, S; Ali, S. (2017). Cloud Computing Risks and Recommendations for Security. International Journal of Latest Research in Science and Technology. Volumen 6. Número 1. p. 52-46.
- Tucker, G; Li, C. (n.d.). Cloud Computing Risks. Universidad de Carolina Este.
- Ross, R; et al. (2018). NIST Special Publication 800-37. Revision 2. Risk Management Framework for Information Systems and Organizations. A System Life Cycle Approach for Security and Privacy. National Institute of Standards and Technology. Departamento de Comercio de Estados Unidos.
- Ross, R; et al. (2012). NIST Special Publication 800-30. Revision 1. Guide for Conducting Risk Assessments. National Institute of Standards and Technology. Departamento de Comercio de Estados Unidos.
- (n.d.). (n.d.). Threat Landscape and Good Practice Guide for Internet Infrastructure. Threat Mind Map. ENISA.
- Brooks, R; et al. (2018). Top Threats to Cloud Computing: Deep Dive. A case study analysis for 'The Treacherous 12: Top Threats to Cloud Computing' and a relative security industry breach analysis. Cloud Security Alliance.
- Hubbard, D; et al. (2010). Top Threats to Cloud Computing V1.0. Cloud Security Alliance.
- Javaid, M. A. (2013). Top Threats to Cloud Computing Security. SSRN Electronic Journal.
- Schwaber, K; Sutherland, J. (2013). La Guía Definitiva de Scrum: Las Reglas del Juego. Scrum.org
- (n.d.). (2017). Chosing KPIs: How to select the right measures for your business. Bellingham Wallace. Disponible en: https://www.bellinghamwallace.co.nz/choosing-kpis-how-to-select-the-right-measures-for-your-business/
- Wilkinson, J. (2015). Why KPIs Are Important. The Strategic CFO. Disponible en: https://strategiccfo.com/why-kpis-are-important/
- Wishart, J.(2020). Why are KPIs Important? Why you Need the Right Key Performance Indicadors. Rhythm Systems. Disponible en: https://www.rhythmsystems.com/blog/5-reasons-why-you-need-kpis-infographic
- (n.d.). (n.d.). A Comprehensive List and Library of Key Risk Indicators with Definitions for Information Technology and Information Security. OpsDog. Disponible en: https://opsdog.com/resources/key-risk-indicators-examples-kris-technology-risk-management/
- (n.d.). (n.d.). What is Plan-Do-Check-Act (PDCA) Cycle? Kanbanize. Disponible en: https://kanbanize.com/lean-management/improvement/what-is-pdca-cycle
- (n.d.). (2019). The Deming Cycle (PDCA) and the constant improvement quality. Twproject. Disponible en: https://twproject.com/blog/deming-cycle-pdca-constant-improvement-quality/

- (n.d.). (2019). The PDCA cycle: more success with the Deming cycle. IONOS. Disponible en: https://www.ionos.com/startupguide/productivity/pdca-cycle/
- (n.d.). (n.d.). Benefits and Challenges of Agile Development. Blueprint. Disponible en: https://www.blueprintsys.com/agile-development-101/agile-benefits-and-challenges
- Novoseltseva, E. (2017). The Benefits You Get By Doing Agile Project Management. Apiumhub. Disponible en: https://apiumhub.com/tech-blog-barcelona/benefits-of-agile-project-management/

Una iniciativa de:

isms forum

CSAES cloud security SPAIN alliance℠