Guía para evaluar un programa de cumplimiento en la Nube

Jorge Wilmar García Gutiérrez [1]

Juan Felipe Gómez Escallón[2]

Resumen

Este artículo está diseñado para ayudar al lector a entender y fortalecer sus iniciativas de cumplimiento en entornos de nube. Para ello, se inicia con la contextualización de la computación en la nube, posteriormente se profundiza en la documentación relacionada con los diferentes componentes de un programa de cumplimiento, así como los desafíos que enfrentan las empresas en su implementación y se finaliza con una propuesta para la evaluación de su programa de cumplimiento. Esto se realiza con la matriz de controles de nube de CSA y con el proceso de gestión del desempeño del marco de gobierno COBIT.

Palabras clave: Auditoría, nube, controles de seguridad, programa de cumplimiento, gestión del desempeño.

[1] Jorge Wilmar García Gutiérrez, Ingeniero de sistemas de la Universidad Salazar y Herrera, Estudiante de especialización en auditoría de sistemas en la Universidad Antonio Nariño, e-mail: jogarcia75@uan.edu.co

[2] Juan Felipe Gómez Escallón, Ingeniero de sistemas de la Universidad de Cundinamarca, Estudiante de especialización en auditoría de sistemas en la Universidad Antonio Nariño, e-mail: jugomez69@uan.edu.co

Abstract

This article is designed to help the reader understand and strengthen their compliance initiatives in cloud environments. To do this, it begins with the contextualization of cloud computing, then goes deeper into the documentation related to the different components of a compliance program, as well as the challenges that companies face in its implementation, and ends with a proposal to evaluating your compliance program. This is done using the CSA cloud controls matrix and the COBIT governance framework performance management process.

Keywords: Audit, cloud, security controls, compliance program, performance management.

Introducción

Hoy por hoy, la cada vez más frecuente acogida de servicios tecnológicos en la nube se ha convertido en eje central de la estrategia organizacional de muchas empresas para mantener su relevancia y supervivencia, frente a sus competidores en el mercado. Esto ha sido posible gracias al despliegue de soluciones de forma global en cuestión de minutos, manteniendo su información replicada, entregando contenido con mayor velocidad y con baja latencia, permitiendo la integración con servicios de terceros, pagando solo por el uso real de infraestructura de cómputo, obteniendo descuentos por mayor consumo de servicios, entre muchos otros.

Sin embargo, a medida que las empresas nacen (como es el caso de muchas Fintech) o migran paulatinamente sus operaciones a entornos en la nube (organizaciones con Datacenter propios o también en ambientes híbridos), emergen grandes desafíos interconectados con: la operación de servicios (Gasto en la nube), el aseguramiento de la información, habilidades requeridas de los diferentes equipos de

trabajo, el gobierno/control, la intimidad/privacidad y la conformidad, entre muchos otros. El compromiso de mantener en curso las operaciones, cumplir con regulaciones y normativas específicas (propias de cada industria y país) y mantener un alto nivel de seguridad de la información y ciberseguridad cada vez cobra mayor relevancia según los reportes de los principales riesgos a nivel mundial para el presente año. (Global Risks Report 2023, 2023)

Con el fin de generar valor a las compañías en su ruta de adoptar/implementar servicios basados en computación en la nube, es fundamental contar con un programa de cumplimiento sólido que garantice que se implementen de manera efectiva sus pilares garantizando una estructura de gobierno sólida que preste especial atención a los procesos, estructuras organizacionales, servicios de tecnología y otros más. La evaluación de dicho programa se vuelve relevante para identificar brechas y vulnerabilidades, que permitirán mejorar la gestión de riesgos, asegurar el cumplimiento regulatorio y permitir la sostenibilidad/rentabilidad de las compañías en el paso del tiempo.

En este artículo entonces, se contextualizan los entornos de computación en la nube, se exploran los componentes, desafíos y oportunidades asociados con la evaluación de programas de cumplimiento en la nube (abordando diferentes estándares y mejores prácticas existentes en la industria), y se proporciona una posible pauta para llevar a cabo la medición de la gestión del desempeño del programa de cumplimiento con COBIT y la matriz de controles de nube de CSA en su versión 4.0.

Metodología

La estrategia metodológica implementada en la redacción del presente artículo, consiste en un acercamiento cualitativo y el enfoque adoptado se basa en el análisis documental de (i) páginas de internet que abordan temas relacionados con auditoría a entornos de Nube tales como ISACA, CSA, NIST entre

muchas otras, (ii) artículos publicados en portales especializados de investigación, tales como Redalyc, Scielo, Dialnet, Elsevier y otros.

Como fuentes secundarias y para dar más soporte a la investigación, se abordaron las siguientes normas, estándares, marcos y mejores prácticas de la industria de forma general, ya que dependiendo de otros factores asociados al cliente de servicios de nube (CSC) estos pueden variar o incluso aumentar: ISO 19011:2018, ISO 31000:2018, matriz de controles de nube, ISO/IEC 27001:2022, ISO/IEC 27017:2015, ISO/IEC 27018:2019, NIST 800.53, COBIT 2019, GDPR, Controles CIS, ITIL y otros.

Resultados y discusiones

¿Qué es la computación en la nube?.

Para evaluar un programa de conformidad de la nube es primordial conocer qué es la nube y todo aquello que la caracteriza. Para ello es necesario comenzar explicando: (i) que son las soluciones de nube, (ii) sus características, (iii) los tipos, (iv) los principales modelos, (v) el alcance de las responsabilidades, (vi) sus beneficios y riesgos, (vii) su gobierno, elementos y complejidades y (viii) estándares, normas y mejores prácticas asociadas.

Una **solución de nube** se define como un modelo tecnológico que habilita: el despliegue desde cualquier parte del globo terráqueo, de forma remota (a través de internet), y en cuestión de minutos, servicios tecnológicos tales como aplicaciones, almacenamiento, procesamiento de datos y cientos más. (Minguillón Roy & Pinar Lorente, 2020)

Su puesta en marcha y gestión **se caracteriza** por estos aspectos: (i) provisionamiento de servicios bajo demanda, es decir que el cliente elige el momento y la cantidad de recursos que desea desplegar y su forma, (ii) acceso a los recursos por intermedio de una conexión por internet, (iii) las capacidades crecientes del habilitador de soluciones de nube (CSP) están puestos a disposición de

múltiples clientes de servicios de nube (CSC) al mismo tiempo, (iv) Elasticidad; es decir que las capacidades solicitadas por el cliente pueden crecer o comprimirse ágilmente, (v) el cliente siempre tiene control de los recursos y está informado constantemente del valor y uso de los mismos, entre muchos otras. (Curiel, y otros, 2020)

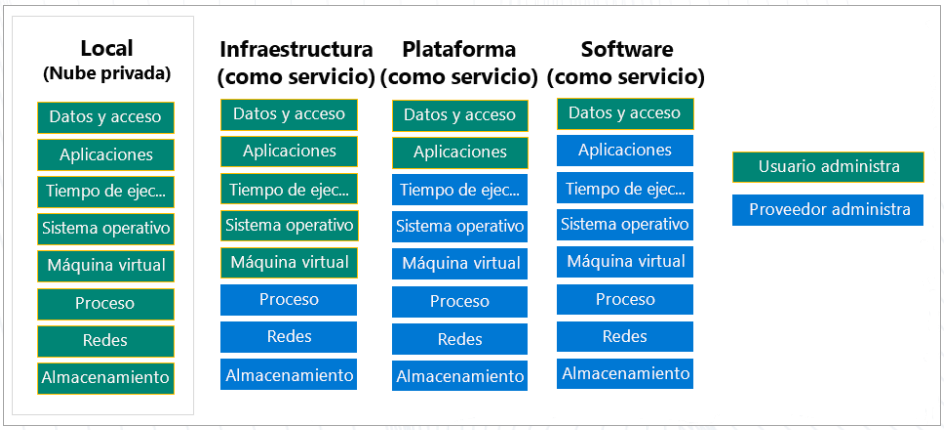
Los **tipos de soluciones** de nube son: **Privada:** es un entorno de computación dedicado exclusivamente a una organización y sus recursos están bajo el control exclusivo de la empresa. **Pública:** el habilitador de servicios de nube administra en su totalidad los recursos de cómputo. Por lo tanto, éste es responsable del mantenimiento de la infraestructura y vela por la Disponibilidad/Accesibilidad, confidencialidad/reserva e integridad/ incorruptibilidad de la información dependiendo de unos niveles de servicio pactados. **Híbrida:** es un entorno donde se mezclan los tipos anteriormente mencionados incluidos los centros de datos On-premises (Centros de datos establecidos en las oficinas de la compañía). (Rodríguez, 2019)

Sus **modelos de despliegue** son: **Infraestructura como servicio (IaaS):** Donde el cliente de servicio de nube adquiere la infraestructura y se encarga de su administración. Es decir, sistemas operativos, aplicaciones, y datos. **Plataforma como servicio (PaaS):** Donde el habilitador de soluciones de nube entrega las plataformas y el cliente administra las aplicaciones y los datos (o información). **Software como servicio (SaaS):** Donde el cliente solo se encarga de consumir los servicios. (Guerola Navarro, 2022)

La **responsabilidad compartida** en el contexto de soluciones en la nube se refiere al ámbito/alcance de responsabilidades entre el CSP y el CSC. Este modelo es intrínseco a todas las soluciones de nube, como IaaS, PaaS y SaaS. La idea principal es que algunas responsabilidades de seguridad y gestión recaen en el CSP, mientras que otras son responsabilidad del usuario.

Para explicarlo fácilmente, se presenta el siguiente gráfico donde se establecen claramente las responsabilidades de las partes:

Figura 1 – Modelo de responsabilidad compartida en entornos de nube.



Nota: El gráfico representa los tipos de responsabilidad de acuerdo al modelo de servicio en la nube.

Tomado de: (Medrano, 2022-2023)

Entre sus principales **beneficios** se encuentran**:** Ahorros en gastos de capital (CAPEX), flexibilidad, escalabilidad, seguridad, rendimiento, colaboración, disponibilidad, agilidad entre muchos otros. Y entre sus **riesgos** se presentan los siguientes: **"**Pérdida" de la gobernanza, protección de la data, eliminación de datos insegura (al finalizar la relación), cumplimiento regulatorio, dependencia, problemas de cadena de suministro, administración de múltiples nubes, falta de habilidades y destrezas, temas jurisdiccionales, transparencia, madurez, sobrecostos por deficiencias en configuración y monitoreo, entre muchos otros. (López & Albanese, 2020)

Para desplegar soluciones es vital tener en cuenta la relación entre tres tipos de gobierno a saber y sus definiciones: **El gobierno corporativo,** es la forma por la cual una empresa constata que las necesidades, estipulaciones, pautas y selecciones de las diferentes partes interesadas se evalúen para determinar si se alcanzan los objetivos empresariales de forma equilibrada y acordada. **Gobierno de TI**, es como se alinea la información y la tecnología al servicio del gobierno corporativo para generar valor.

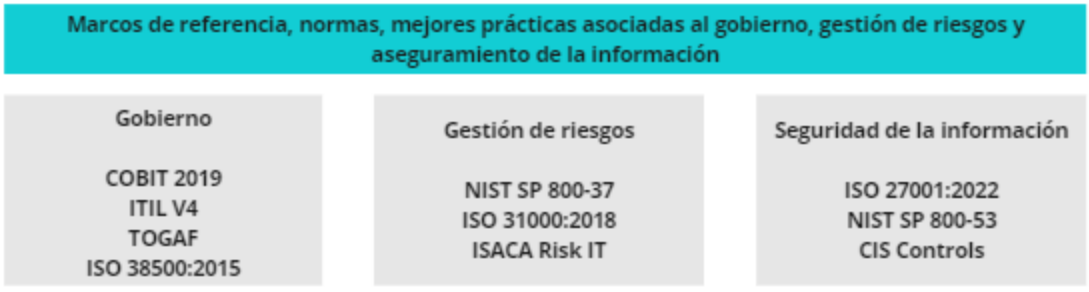
Gobierno de nube, se refiere a la creación y materialización de políticas, procesos y medidas para administrar los servicios en la nube dentro de una organización, buscando garantizar la coherencia con las metas estratégicas de la compañía, gestionando eficientemente los recursos, asegurando el cumplimiento regulatorio, y gestionando los riesgos asociados con la protección y confidencialidad de la información. (El impacto del gobierno corporativo y sus tendencias emergentes, 2023)

Ahondando un poco más en el gobierno de nube, se deben considerar los siguientes elementos y complejidades: (i) Gobernanza: Roles y responsabilidades, (ii) arquitectura empresarial y cultura, (iii) seguridad: Riesgos de seguridad (evaluaciones), cumplimiento y auditoría. (iv) Operaciones de TI: servicios desplegados y TI Oculta, (v) Infraestructura de TI: interconexión de servicios, (vi) Administración de redes. (vii) identidades y accesos: control de accesos, (viii) virtualización, (ix) Resiliencia empresarial y recuperación frente a eventos catastróficos, (x) Propietarios de productos, servicios y sistemas de información y (xi) administración de finanzas y contratos. (Ekuan, y otros, 2023)

La adopción de marcos, estándares, normas y mejores prácticas en el despliegue de soluciones en la nube conlleva diversas ventajas tales como: (i) tener un enfoque ampliamente validado que facilita el despliegue y gestión de recursos en la nube. (ii) contar con guías sólidas, que mantienen coherencia y uniformidad en las operaciones, aspecto primario para la eficiencia y la consistencia, (iii) estos instrumentos ofrecen directrices puntuales en materia de seguridad, (iv) reducir riesgos, amenazas, vulnerabilidades y ataques, ayudando a mantener la exactitud, accesibilidad y reserva de los datos, (v) la compatibilidad con estándares y normas reconocidas, pues al adherirse a estos, las organizaciones pueden asegurar la interoperabilidad y la portabilidad de las soluciones en la nube, (vi) la eficiencia operativa se ve optimizada por la asignación adecuada de recursos hasta estrategias de escalabilidad y gestión de carga de trabajo. (Torres, s.f.)

A continuación, se relacionan marcos de referencia, normas y mejores prácticas asociadas al gobierno, gestión de riesgos y aseguramiento de la información existentes.

Figura 2 – Marcos de referencia, normas, modelos y estándares asociados al gobierno, gestión de riesgos y aseguramiento de información



Nota: Elaboración propia.

Componentes de un programa de cumplimiento de nube

Continuando con la evaluación de un programa de conformidad de la nube, lo siguiente que se debe acometer es: (i) Abordar consideraciones clave como el cumplimiento normativo, la atención a los contratos, Acuerdos de Nivel de Servicio (ANS) y Términos de Servicio (ToS), el entendimiento del modelo de responsabilidad, los posibles incumplimientos y las evaluaciones periódicas la consistencia del programa. (ii) Tratar el núcleo del programa: es decir, Interesados y comprender el contexto organizacional, los marcos legales que rijan las operaciones de la compañía, la evaluación de riesgos asociados a los servicios desplegados, (iii) La construcción de los componentes del programa teniendo en cuenta: La definición de procesos, arquitecturas organizacionales, principios, políticas y marcos regulatorios, la gestión de la información, la promoción de una cultura ética y comportamiento responsable, así como las personas, sus habilidades y competencias y los servicios desplegados. (iv) Los requisitos legales y los marcos específicos a los programas de conformidad en la nube asociados a estos.

Las diversas **consideraciones** que un programa de cumplimiento en la nube debe abordar, abarcan un amplio espectro de reflexiones críticas que son fundamentales para garantizar la conformidad, la seguridad y el control efectivo de riesgos en contextos asociados a soluciones en la nube.

- El **cumplimiento normativo** afecta el despliegue de productos o servicios de nube. El análisis debe ahondar en los impactos y desafíos, considerando factores como la ubicación geográfica donde se alojan los datos, la protección de la privacidad (Datos personales identificables o información de tarjetas de crédito), el control de identificaciones y autorizaciones (Mínimo privilegio), y las regulaciones propias de la industria del CSC (Gobierno, financiero o salud).
- **Los contratos, acuerdos de niveles de servicio (ANS) y términos del servicio (ToS)** son documentos que definen los parámetros y condiciones bajo los cuales se proporcionan y utilizan los servicios en la nube (ejemplo: Soporte técnico, subcontratación). Estos documentos no solo afectan las expectativas y obligaciones de las partes, sino que también especifican las medidas y niveles de seguridad, tiempos de respuesta, los compromisos de privacidad, así como los protocolos para gestionar soportes, capacitaciones, incidentes y posibles incumplimientos.
- **El modelo de responsabilidad** es otro componente crucial (anteriormente explicado), ya que establece claramente el alcance de las responsabilidades de seguridad entre el cliente y el habilitador de soluciones en la nube. Dependiendo del esquema de prestación del servicio (IaaS, PaaS o SaaS), algunas responsabilidades relacionadas con la seguridad, el monitoreo, rendimiento, mantenimiento y la gestión de datos pueden recaer en el CSP, mientras que otras pueden hacerlo sobre el CSC.
- En caso de **incumplimientos**, el programa de cumplimiento debe contener información clara y precisa para abordar estas situaciones (Documentación). Esto implica la implementación de medidas correctivas, su alcance (RTO, RPO entre otros), la resolución de disputas, el alcance de las sanciones, las líneas de comunicación, notificaciones a reguladores, notificación a partes afectadas y la mitigación de riesgos para evitar nuevas ocurrencias, así como la evaluación de daños y pérdidas o la rescisión del contrato.

- En cuanto a las **evaluaciones**, el programa de cumplimiento debe incluir varios tipos. Estas evaluaciones pueden abarcar auditorías al CSP o al CSC (como por ejemplo al Gobierno, a las configuraciones, accesos), revisiones de cumplimiento normativo, evaluaciones de riesgos de seguridad, de rendimiento y de impacto a privacidad entre muchas otras. Estos procesos son base para monitorear, evaluar y mejorar continuamente el rendimiento de las salvaguardas (Hardening) y garantizar que se mantenga el cumplimiento legal y normativo aplicables. (¿Qué es el Cumplimiento de la Nube?, s.f)

El **núcleo** de un programa de conformidad en la nube abarca diversos aspectos para otorgar una gestión efectiva, sostenible y equilibrada en el cambiante entorno tecnológico. A continuación, se explican algunos de los más relevantes. (Ekuan, y otros, 2023)

- L**os interesados**, teniendo muy en cuenta que ellos poseen un interés variable en el despliegue, operación y mantenimiento de servicios en la nube. Estos interesados pueden ser los usuarios finales y clientes de la empresa, los propios empleados, la comunidad, grupos sociales, grupos ambientales, proveedores de productos y servicios complementarios y finalmente los reguladores. La comprensión y correcta gestión de sus expectativas y necesidades es muy importante para elegir las políticas, procesos, responsabilidades y demás del programa.
- **El contexto organizacional** se erige como otra columna, involucrando la evaluación y comprensión detallada de las circunstancias del ámbito organizacional. Esto implica tener en cuenta varios tipos de análisis que se encuentran en el entorno empresarial tales como: Matriz PESTEL, DOFA, Kraljic, Fuerzas de Porter y muchas más para adaptar el programa de cumplimiento a la realidad de la empresa.
- **El cumplimiento legal**, toma la identificación y adhesión a las leyes y regulaciones pertinentes asociadas con la ubicación geográfica de la organización, así como el sector (HIPAA, PCI-DSS)

y la índole de los servicios habilitados en la nube. Esto incluye normativas específicas de importación y exportación (ITAR), derechos de autor, información financiera (Ley SOX, IFRS) privacidad (GDPR), seguridad de datos, y otros requisitos legales aplicables (Cadenas de custodia). Aquí toma especial relevancia el proceso de cumplimiento continuo.

- **La operación de servicios contratados** en la nube, conlleva la instauración de lineamientos, prácticas y protocolos que aseguren la operación segura, eficiente y conforme las políticas empresariales y el alcance del producto y servicio contratado. Incluye la gestión de accesos, la medición del desempeño, la actualización de componentes, el mantenimiento, actualización y reemplazo de recursos, el aseguramiento de datos, la seguridad de la red, y otras prácticas operativas primarias.
- Por último, la **evaluación de riesgos** es sustancial para anticipar/prevenir, identificar/detectar y gestionar/corregir los riesgos asociados con Adquisición y mantenimiento de soluciones en la nube. Implica el análisis cualitativo o cuantitativo, evaluación y respuesta continua de amenazas, vulnerabilidades, el impacto de eventos no evaluados en la seguridad y el cumplimiento, así como el mejoramiento continuo. Para ello es muy importante que la empresa determine indicadores estratégicos tales como el apetito, la tolerancia y la capacidad de riesgos.

La construcción del programa de conformidad en la nube, involucra los siguientes componentes.(Cómo crear un programa de cumplimiento efectivo: importancia, elementos y primeros pasos, 2022)

- **Procesos**, que son descritos como un sistema estructurado de métodos y acciones esenciales para lograr metas, y generar los resultados orientados hacia la materialización de todos los objetivos del proceso de TI y por consecuencia del negocio. Estos constituyen un componente esencial para

identificar, evaluar y mitigar posibles amenazas a la protección y la incolumidad de los datos en entornos de nube. Aquí toma especial relevancia el proceso de gestión de riesgos.

- **Las arquitecturas organizativas** son los cuerpos encargados del proceso resolutivo en la entidad, y son definidas a través de las Matrices RACI, las cuales presentan la asignación de compromisos, autoridades y papeles a personificar en relación con las actividades que engloba cada proceso en el ámbito de la conformidad en la nube. Esto implica la supervisión y ejecución efectiva de las políticas, procesos y procedimientos y demás normas o lineamientos establecidos.
- **Los principios**. Son una guía práctica que representa y manifiesta el comportamiento deseado para la conducción cotidiana en la empresa. Estos detallan de manera inconfundible los valores inquebrantables de la empresa**; las políticas** ofrecen una pauta para materializar los principios y su repercusión en la toma de decisiones; y finalmente **los marcos** suministran a la dirección de una organización, pautas y artefactos que faciliten una apropiada gestión y gobernanza. Estos tres elementos, forman el marco que guía el programa de auditorías y la gestión del cumplimiento regulatorio. Estas directrices proporcionan a su vez, la base para evaluar el cumplimiento de leyes, estándares y regulaciones propias de la actuación en la nube.
- **La información**, es imprescindible para la operación, desarrollo y trascendencia de la empresa, y su buena administración; en el nivel ejecutivo es el componente esencial para la empresa (Por tanto, es altamente riesgoso). La gestión de la información incluye la protección, clasificación y manejo adecuado de la información crítica, asegurando su disponibilidad, integridad y confidencialidad.
- **La cultura, ética y comportamiento** se definen como características de las personas y de la organización, visto como factor clave de éxito de las actividades de gobernanza y gestión. Abarca la totalidad de comportamientos personales y grupales dentro de la empresa tales como hábitos, costumbres, valores y propósito. Lo cual influye directamente en la conformidad de la nube, así como en la protección y gobernabilidad de riesgos.

- **Las personas, habilidades y competencias,** son necesarias para la culminación exitosa de todos los quehaceres de la organización, y más cuando se requiere adoptar las decisiones idóneas y las medidas necesarias para el éxito de la empresa, en este particular, los auditores son esenciales para llevar a cabo evaluaciones efectivas de cumplimiento. Se requiere un personal capacitado, dispuesto y competente para comprender, analizar y evaluar las complejidades de la nube y realizar auditorías exhaustivas.
- **Las funciones, habilitadores y soluciones de software** forman parte de la evaluación de operaciones en un entorno de nube. Esto incluye:
    - **Elección del CSP**. Tratando temas como: (i) seguridad y cumplimento a través de evaluaciones de terceros y sus prácticas de seguridad, (ii) transparencia en la entrega de información. (incidentes conocidos), (iii) evaluaciones de resiliencia, (iv) experiencia de cliente, a través de comentarios y reseñas. (v) cumplimiento normativo, evaluando si cumple con programas de implementación de controles de nube, entre otros. (¿Cómo se elige un proveedor de servicios en la nube?, s.f.)
    - **Eficiencia operativa.** Abordando temas como: (i) servicio ofrecido: contratos y condiciones de uso, auditorías, evaluaciones de riesgos, rendimiento y monitoreo, entre otros. (ii) proveedor/habilitador: Reputación, auditorías de terceros, madurez, habilidades, postura de seguridad y cumplimiento, entre otros. (Orin, 2023)
    - **La confianza en la nube:** establecida sobre (i) la transparencia del habilitador de servicio de nube: es decir; la capacidad y disposición del habilitador para proporcionar información clara, completa y accesible a sus clientes sobre aspectos relacionados con la oferta de servicios (Acuerdos de niveles de servicio, reputación, certificaciones emitidas por terceros, evidencias, postura de seguridad y otras más). (ii) aseguramiento: capacidades asociadas a la recuperación de desastres, continuidad de las operaciones y seguros. (iii) responsabilidad: asociada a la capacidad de responder como solidario encargado de la información y su seguridad. (Balboni, Mccorry, & Snead, 2009)

La prestación de servicios de nube, implica prestar atención a una serie de requisitos legales para garantizar la operación legal y segura en el entorno tecnológico. La diversidad de regulaciones abarca desde la protección de datos personales hasta normativas sobre comercio electrónico, telecomunicaciones, delitos informáticos y seguridad de la información, entre muchos otros. La comprensión y aplicación de estas regulaciones también fortalecen la confianza de los clientes de la empresa y contribuyen al desarrollo de un entorno digital ético y legal en el mundo. La adaptación constante a cambios normativos y la consulta de asesoramiento legal son muy importantes para mantener la conformidad y la integridad en la prestación de servicios de nube.

A continuación, se exponen algunos requisitos legales, asociados a programas de cumplimiento. (Curiel, y otros, 2020)

Figura 4 – Requisitos legales y reglamentarios, asociados a programas de cumplimiento

Nota: Elaboración propia

Para abordar efectivamente los desafíos de un programa de cumplimiento, es prioritario contar con un marco sólido que guíe la evaluación y el cumplimiento normativo. En este sentido, diversos marcos, normas, estándares y mejores prácticas han sido desarrollados para establecer directrices sobre el aseguramiento de los datos en la nube. Cada uno de estos enfoques ofrece una perspectiva única,

permitiendo a las organizaciones adaptar su estrategia de cumplimiento según sus necesidades específicas y el entorno normativo en el que operan.

A continuación, se presentan los marcos de controles comúnmente adoptados para programas de cumplimiento en la nube. (Curiel, y otros, 2020)

Figura 3 – Marcos de controles para programas de conformidad en la nube

Nota: Elaboración propia

CCM de CSA. Es un marco de seguridad elaborado, potenciado y madurado por la Cloud Security Alliance (CSA). La CSA es una entidad dedicada a promover las prácticas sobresalientes en materia de resguardo de soluciones habilitadas en la nube. Por lo tanto, CCM brinda una serie de salvaguardias de seguridad y principios relacionados con la nube que sirven como un estándar para ayudar a las organizaciones a evaluar el riesgo de protección de los habilitadores de soluciones en la nube. (Cloud Controls Matrix (CCM), s.f), se elige estudiar a fondo el presente marco, debido a que intrínsecamente tiene vínculos con otras normas ISO 27001:2913, ISO 27002:2013, ISO 27017:2015, con ISO 27018:2019 y con la versión anterior de CCM por lo cual es más mucho más amplio.

Este marco es valioso porque está dirigido a diversos públicos, incluyendo habilitadores de soluciones en la nube (CSP), contratantes de soluciones en la nube (CSC), CISO´s, arquitectos, auditores, reguladores y organismos de cumplimiento.

- **Los habilitadores (CSP)** lo utilizan para: tener una lista detallada de requerimientos, mejorar sus prácticas de seguridad, normalizar expectativas en seguridad.
- **Los clientes (CSC)** para: tener información de prácticas para la nube y reconocidas por la industria, ayudar a valorar/atestar la seguridad de los habilitadores de soluciones en la nube y complementar o alinear prácticas realizadas con otros estándares de la industria.
- **Los arquitectos de soluciones de nube** pueden utilizar la CCM como una guía detallada para diseñar productos y servicios seguros y resilientes en la nube.
- **Los auditores**, lo utilizan para tener un fundamento detallado y criterios de evaluación para realizar auditorías exhaustivas, permitiendo valorar el rendimiento de las medidas de amparo desplegadas por los habilitadores de soluciones en la nube.
- **Los reguladores y organismos de cumplimiento**, pueden utilizar la CCM como referencia para evaluar y garantizar el cumplimiento normativo en entornos de nube de las organizaciones.

Guía para evaluar un programa de conformidad en la nube

Los programas de cumplimiento a entornos de nube se ha vuelto una necesidad empresarial recurrente, debido a que el despliegue de soluciones en la nube se ha convertido en una práctica común. La necesidad de evaluar componentes en estos entornos ha llevado a reconocer la importancia estratégica de los programas de conformidad en la nube. Este proceso no solo garantiza la seguridad de los datos, sino que también asegura el cumplimiento de normativas específicas. La complejidad propia de los ambientes de nube, destaca la necesidad de una auditoría sistemática para mitigar riesgos, optimizar recursos y mantener estándares de calidad. En este ámbito, la auditoría no solo es una herramienta de

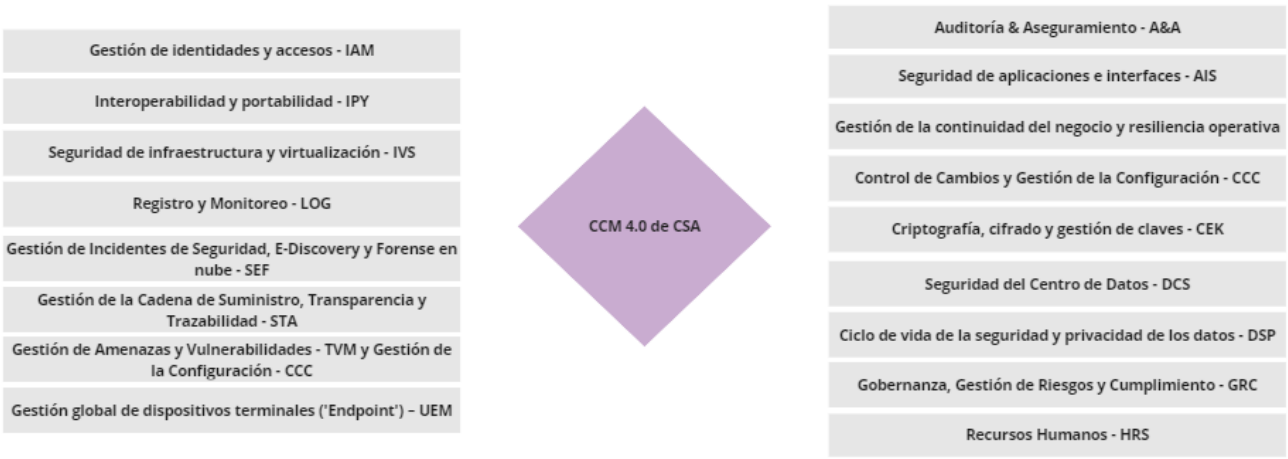
verificación, sino también un pilar fundamental para la confianza de los clientes, la resiliencia del negocio y la adaptabilidad en entornos de constante evolución.

La Cloud Controls Matrix (CCM) nace como una opción para calificar el estado de cumplimiento en la implementación de controles de nube y por ende el grado de implementación del programa de cumplimiento de nube.

La CCM se divide en categorías que agrupan controles de seguridad relacionados en el contexto de soluciones en la nube. Cada dominio aborda un área específica de consideración para afianzar la seguridad. Estos dominios sirven para organizar y estructurar los controles de seguridad, facilitando la comprensión y aplicación de prácticas seguras en la nube. Cada dominio contiene controles bastante específicos que proporcionan pautas para mitigar riesgos y garantizar la conformidad de la información en la nube.

CCM cuenta con 17 dominios (Consistentes en 197 controles) los cuales son:

Figura 5 – Dominios CCM 4.0 de CSA



Nota: Elaboración propia

La gestión del desempeño en COBIT (CPM) constituye un componente esencial en un sistema donde convergen la dirección y la conducción (Gobierno y gestión). Este término abarca diversas actividades y métodos, reflejando la efectividad de ambos estamentos a través de las capacidades inherentes a las medidas desplegadas, además, indica cómo se pueden optimizar para alcanzar el nivel necesario. (COBIT 2019 Framework: Introduction & Methodology, 2019)

Figura 6 – Principios de desempeño de COBIT 2019

Nota: Elaboración propia

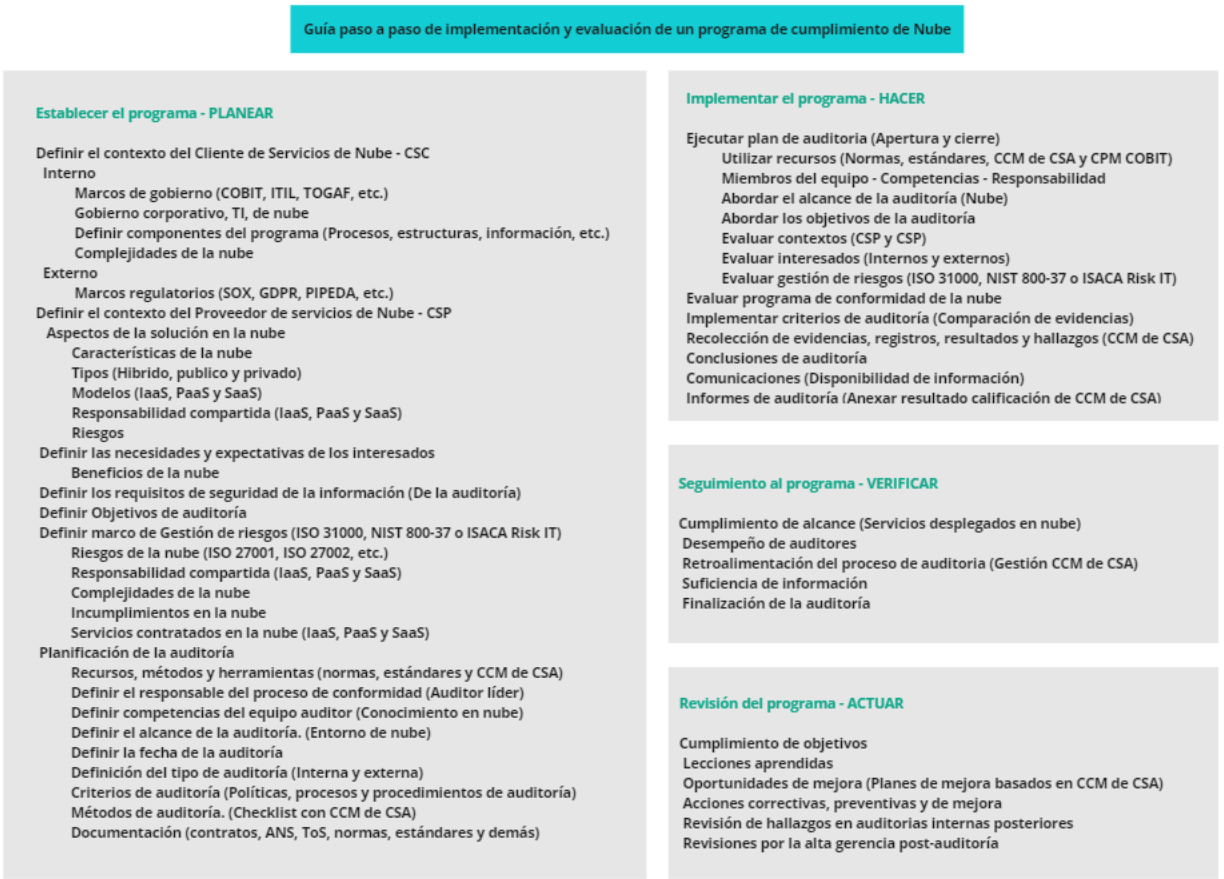
La capacidad puede alcanzar diversos niveles, y estos pueden expresarse a través de diversas calificaciones (Gorgona, 2021). El conjunto de calificaciones disponible varía según el contexto en el que se lleva a cabo la evaluación de rendimiento:

- Los métodos convencionales usan calificaciones binarias de cumple/no cumple o similares.
- Los métodos menos convencionales funcionan mejor con un listado de calificaciones más amplio, como el siguiente:
  - Íntegramente - El nivel de cumplimiento es superior al 85%
  - Ampliamente - El nivel de cumplimiento está entre el 51% y el 85%.
  - En parte - El nivel de cumplimiento está entre el 16% y el 50%
  - Baja- El nivel de cumplimiento es inferior al 15 por ciento.

Por lo tanto, se puede utilizar el CPM sobre los diferentes dominios de la CMM, para establecer el nivel de capacidad/adopción (Baja, En parte, Ampliamente, Íntegramente) de cada uno de los 17 dominios con sus 197 controles y el estado de madurez del cliente de servicios de nube (CSC) y del habilitador de servicios de nube. (CSP)

Así pues, se presenta en la siguiente imagen, la guía condensada para implementar y evaluar un programa de conformidad en la nube con CCM de CSA y CPM, basado en la norma ISO 19011:2018 y con los elementos presentados en el cuerpo del presente artículo.

Figura 7 – Guía de implementación y evaluación del programa de desempeño en la nube



Nota: Elaboración propia

Conclusiones

1. Se comprobó que una guía efectiva para evaluar un programa de cumplimiento en la nube debe fomentar un enfoque holístico. Esto implica considerar aspectos técnicos, legales, de seguridad y de rendimiento en conjunto. La evaluación integral garantiza que no se pasen por alto aspectos críticos y proporciona una visión completa del estado de cumplimiento.
2. La guía debe destacar la importancia de la adaptabilidad y la evolución continua del programa de cumplimiento en la Nube. Las entidades deben estar preparadas para ajustar y mejorar sus prácticas de cumplimiento con el fin de ajustarse a las evoluciones tecnológicas y en las regulaciones.
3. La integración de estándares reconocidos, como CCM y la gestión del desempeño de COBIT, permiten establecer un marco para evaluar el cumplimiento. Al vincular estos estándares, se proporciona un método estructurado para medir el desempeño. Esta integración no solo mejora la eficacia de la evaluación, sino que también establece una base sólida para mejoras continuas en el programa.

Referencias

Azure. (s.f.). Recuperado el 26 de 09 de 2023, de https://azure.microsoft.com/es-es/resources/cloud-computing-dictionary/choosing-a-cloud-service-provider

Balboni, P., Mccorry, K., & Snead, D. (2009). *Enisa*. Recuperado el 17 de 10 de 2023, de https://www.enisa.europa.eu/topics/risk-management/files/deliverables/cloud-computing-risk-assessment-spanish

Cloud Security Alliance. (s.f). Recuperado el 25 de 10 de 2023, de https://cloudsecurityalliance.org/research/cloud-controls-matrix/

Curiel, G., Mora Lavin, J., Martínez Bermejo, J. M., Coz, J. R., Avelino, M., & Feito, M. (2020). *Isaca Madrid*. Recuperado el 1 de 10 de 2023, de https://higherlogicdownload.s3.amazonaws.com/ISACA/b6277216-42ab-46b4-91b4-518d4c513528/UploadedImages/Cuadernos_de_ISACA_Madrid/Auditoria_Cloud_ISACA_def.pdf

Ekuan, M., Petersen, T., Sherer, T., Moore, G., Buck, A., Wray, S., . . . Vilaysom, S. (28 de 03 de 2023). *Azure*. Recuperado el 1 de 10 de 2023, de https://learn.microsoft.com/es-es/azure/well-architected/

Ekuan, M., Zimmergren, T., Moore, G., Buck, A., Coulter, D., Mabee, D., . . . Rachkidi, F. (11 de 07 de 2023). *Microsoft Ignite*. Recuperado el 03 de 10 de 2023, de https://learn.microsoft.com/es-es/azure/cloud-adoption-framework/organize/cloud-governance

Escuela Europea de Excelencia. (15 de 03 de 2022). Recuperado el 08 de 10 de 2023, de https://www.escuelaeuropeaexcelencia.com/2022/03/como-crear-un-programa-de-cumplimiento-efectivo-importancia-elementos-y-primeros-pasos/#:~:text=Un%20programa%20de%20cumplimiento%20es,no%20son%20de%20talla%20%C3%BAnica.

Gorgona, L. (28 de 12 de 2021). *ISACA*. Recuperado el 01 de 11 de 2023, de https://www.isaca.org/es-es/resources/isaca-journal/issues/2021/volume-6/building-a-maturity-model-for-cobit-2019-based-on-cmmi

Guerola Navarro, V. (10 de 02 de 2022). *Universidad Politecnica de Valencia*. Recuperado el 16 de 10 de 2023, de https://riunet.upv.es/handle/10251/180717

ISACA. (2019). Recuperado el 30 de 10 de 2023, de https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004Ko9DEAS

López, M. d., & Albanese, D. (12 de 12 de 2020). *Researchgate*. doi:https://doi.org/10.24215/27188647e001

Medrano, A. (2022-2023). *Aitor-Medrano*. Recuperado el 15 de 10 de 2023, de https://aitor-medrano.github.io/iabd2223/cloud/01cloud.html#plataformas-cloud

Minguillón Roy, A., & Pinar Lorente, E. (2020). *Revista auditoría pública*. Recuperado el 20 de 10 de 2023, de https://publicaciones.4tintas.es/ccuentas/auditoriapublica75/files/assets/common/downloads/auditoriapublica75.pdf?uni=011ba6de4d73ca4e11fee5f993958142

Orin, E. (13 de 06 de 2023). *Izertis*. Recuperado el 4 de 10 de 2023, de https://www.izertis.com/es/-/blog/gobernanza-de-la-nube-o-como-sacar-el-maximo-provecho-del-cloud-computing

Rodríguez, G. S. (2019). *Dialnet*. doi:http://dx.doi.org/10.21503/lex.v17i23.1674

Sydle. (21 de 09 de 2023). Recuperado el 05 de 10 de 2023, de https://www.sydle.com/es/blog/esg-gobierno-650c4f96118e9e7c1a5d0b6e

Torres, C. (s.f.). *Webdox*. Recuperado el 07 de 11 de 2023, de https://www.webdoxclm.com/blog/normas-iso-de-ciberseguridad-27001-27701-27017-27018-27032

Trendmicro. (s.f). Recuperado el 01 de 10 de 2023, de https://www.trendmicro.com/es_mx/what-is/cloud-security/cloud-compliance.html

World Economic Forum. (11 de 01 de 2023). Recuperado el 15 de 10 de 2023, de https://www.weforum.org/publications/global-risks-report-2023/in-full/1-global-risks-2023-today-s-crisis/#1-global-risks-2023-today-s-crisis