AUDITORÍA INTERNA

LA FÁBRICA DE PENSAMIENTO
INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA

Auditoría Interna de la gestión operativa del Cloud

The Institute of Internal Auditors

Instituto de Auditores Internos de España

El INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA es una asociación profesional fundada en 1983, cuya misión es contribuir al éxito de las organizaciones impulsando la Auditoría Interna como función clave del buen gobierno. En España cuenta con más de 3.500 socios, auditores internos en las principales empresas e instituciones de todos los sectores económicos del país.

LA FÁBRICA DE PENSAMIENTO es el laboratorio de ideas del Instituto de Auditores Internos de España sobre gobierno corporativo, gestión de riesgos y Auditoría Interna, donde participan más de 150 socios y profesionales técnicos expertos.

AUDITORÍA INTERNA

OBSERVATORIO SECTORIAL

PRÁCTICAS DE BUEN GOBIERNO

BUENAS PRÁCTICAS EN GESTIÓN DE RIESGOS

El laboratorio trabaja con un enfoque práctico en la producción de documentos de buenas prácticas que contribuyan a la mejora del buen gobierno y de los sistemas de gestión de riesgos en organizaciones de habla hispana. Además de desarrollar contenido, fomenta el intercambio de conocimientos entre los socios.

ENCUENTRA TODOS LOS DOCUMENTOS DE LA FÁBRICA EN www.auditoresinternos.es

AUDITORÍA INTERNA

LA FÁBRICA DE PENSAMIENTO
INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA

Auditoría Interna de la gestión operativa del Cloud

Enero 2025

MIEMBROS DE LA COMISIÓN TÉCNICA

COORDINACIÓN:

Iván Casacuberta Prats, CIA, CISA, CISM, CCAK, CISSP, CCSP, CDPP. CAIXABANK.

Roberto Avilés Blesa, CISA, CISM, COSO-CI, CISSP, ISO27001, ITIL Expert. IBERDROLA.

David Canales Castellanos, CISA, COSO-CI. REPSOL.

David Cons Pombo, CISA. INDITEX.

Rodrigo Feito Blanco, CISA, ISO27001, ISO27017, ISO42001. PWC.

Vanesa Gómez Fernández, ISO27001, ISO22301, ISO/IEC27017, ENS. BBVA, IT Risk & Cybersecurity.

Melania Haro Peredo, CISA, CISM, CRISC. DELOITTE.

Jonathan Laguna Ciudad, CISM. EY.

Francisco Martín Vázquez, CEH, COSO-CI. TELEFÓNICA.

Roger Pérez Movilla, CISA, CISM, CRISC, ISO 27001. BDO.

Luis Reinoso Tello, CISA, CISM. FORVIS MAZARS.

Pau Serra Morales, CISA, CRISC, CFS-EU, ISO22301. BANCO SABADELL.

The Institute of Internal Auditors

Instituto de Auditores Internos de España

Auditoría Interna constituye una función clave dentro de cualquier organización, ya que ofrece garantías de la eficacia de sus procesos de gobierno, control y gestión de riesgos, proporcionando valor y un nivel de seguridad adecuado a los órganos de dirección y supervisión. En este sentido, Auditoría Interna debe estar al día de las tendencias y desafíos que afectan a su actividad, entre los que se encuentra el uso cada vez más extendido de servicios en la nube.

Los servicios en la nube ofrecen numerosas ventajas a las organizaciones, tales como la reducción de costes, la escalabilidad, la flexibilidad, la innovación o la optimización de los recursos. Sin embargo, también implican una mayor complejidad, incertidumbre y exposición a amenazas que requieren una evaluación y mitigación de los riesgos asociados que sea adecuada.

La externalización de datos, de aplicaciones o de infraestructura a los proveedores de servicios en la nube supone un cambio significativo en el modelo de negocio y de gestión de las organizaciones, que afecta a aspectos clave como la seguridad, la privacidad, la continuidad, la calidad o el cumplimiento con la legislación y/o la regulación de la compañía. Por ello, Auditoría Interna debe asegurar que las organizaciones cuentan con los mecanismos necesarios para gestionar todos estos aspectos y para supervisar el cumplimiento de los acuerdos de nivel de servicio establecidos con los proveedores.

El papel del auditor interno en relación con las actividades externalizadas a entornos cloud depende del tipo de externalización adoptada, que suele clasificarse en cuatro modelos: IaaS, PaaS, SaaS y FaaS. Cada uno de estos modelos implica un diferente nivel de responsabilidad compartida entre el proveedor y el cliente, así como un diferente alcance y grado de complejidad para los trabajos y revisiones efectuadas por Auditoría Interna.

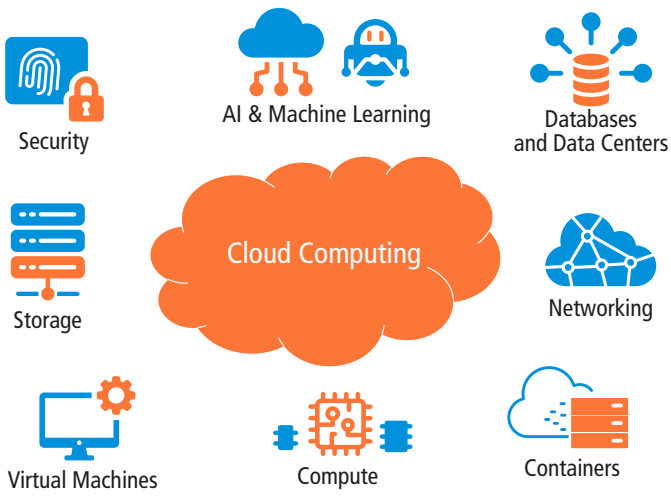
En este documento se analizan los modelos de externalización a entornos cloud y sus principales riesgos y beneficios, así como las mejores prácticas y recomendaciones para la realización de auditorías internas eficaces y eficientes en entornos cloud. El objetivo del documento es proporcionar una guía útil y práctica para los auditores internos, que les ayude a afrontar con éxito los retos que plantea esta parte del proceso de transformación digital de las organizaciones y a contribuir a la mejora continua de su desempeño.

Contenido

Introducción

¿PUEDEN LAS MÁQUINAS PENSAR?

La denominación nube *(cloud* en inglés), es la metáfora del icono con el que se representaban las infraestructuras de Internet en los diagramas de flujo. Se trata de una generalización para referirse a la externalización de datos, aplicaciones o infraestructura.



En los últimos años ha surgido un modelo de servicios que tiene su origen en los años 60 del siglo XX, cuando comenzaron los primeros servicios en la nube con el acceso a sistemas informáticos centralizados a través de terminales, si bien su mayor impulso comenzó en la década del 2000 con los modelos de "software como servicio" (en adelante modelos SaaS[1] por sus siglas en inglés). La popularización de los servicios en la nube se inició cuando Amazon Web Services (AWS) lanzó su plataforma de servicios en la nube en el año 2006, ofreciendo servicios de "infraestructura como servicio" (en adelante modelos IaaS[2] por sus siglas en inglés) y con el tiempo se han ido añadiendo nuevos servicios en la nube como "plataforma como servicio" (en adelante modelos PaaS[3] por sus siglas en inglés), "funciones como servicio" (en adelante modelos FaaS[4] por sus siglas en inglés), etc.

La forma en la que muchas organizaciones han decidido aproximarse a la nube es bajo un modelo de despliegue conocido como nube híbrida, que combina servicios de computación, almacenamiento, etc. en distintos entornos como nubes públicas, nubes privadas y centros de datos *on-premise* de las propias organizaciones, estos términos se desarrollan posteriormente, a lo largo del documento. Este modelo permite una adaptación paulatina a la nube y beneficiarse de lo mejor de los

1. *Software as a Service.*
2. *Infraestructure as a Service.*
3. *Platform as a Service.*
4. *Function as a Service.*

distintos entornos, pero también incrementa la complejidad al tener que gobernar distintos entornos que interoperan entre sí.

Las principales **ventajas y oportunidades** de los servicios en la nube son:

- **Escalabilidad y gestión de la capacidad** - permiten escalar recursos fácilmente según las necesidades del usuario.
- **Agilidad y flexibilidad** - permite a las empresas adaptarse rápidamente a los cambios en el mercado y a las necesidades del negocio.
- **Acceso global** - son accesibles a través de Internet desde cualquier lugar del mundo.
- **Coste / beneficio** - es menos costoso de mantener que una infraestructura *on-premise*.
- **Gestión simplificada y actualizaciones automática** - gestión y actualizaciones de la infraestructura de manera trasparente para los clientes.
- **Respaldo y recuperación de datos** - capacidades de respaldo y recuperación de datos integradas.

Los principales **riesgos** de los servicios en la nube son:

- **Pérdida de gobernabilidad** - la cesión de control al proveedor, puede producir una pérdida de la gobernabilidad propia, así como una mayor dificultad de acceso directo a la supervisión de los servicios en la nube, incluyendo las actividades de aseguramiento por parte de los equipos de auditoría interna.
- **Coste / beneficio** - en algunas ocasiones, a largo plazo, el coste de mantener una infraestructura en la nube puede ser superior al coste que supondría *on-premise*.
- **Cumplimiento normativo** - almacenar datos en la nube puede plantear desafíos en términos de cumplimiento normativo, especialmente en sectores altamente regulados como la salud, el financiero o de gobierno.
- **Privacidad** - los clientes deben confiar en que los proveedores protejan adecuadamente sus datos y cumplan con las regulaciones de privacidad aplicables.
- **Ineficiente borrado de información** - la compartición de infraestructuras en la nube puede hacer inviable seguir la Política de Seguridad en materia de borrado de datos.
- **Fallo de aislamiento** - la multiprestación de servicios por parte del proveedor, podría ocasionar problemas en los mecanismos que separan el almacenamiento, memoria, etc.
- **Seguridad de la información** - la información almacenada en la nube puede estar expuesta a ciberataques, brechas de seguridad o accesos no autorizados.
- **Dependencia de proveedores** - los clientes con una elevada vinculación a determinados proveedores (ya sea por concentración de servicios o por criticidad de los mismos), están más expuestos a estos ante situaciones como errores operacionales o de seguridad significativos, sanciones o bloqueos internacionales, quiebra económica del proveedor, etc.

Todo este auge de servicios en la nube, con los nuevos riesgos y retos derivados, supone un reto para los auditores internos, que deben contar con una serie de competencias adecuadas para aportar valor a las organizaciones y contribuir a la calidad, la eficiencia y

El auge de los servicios en la nube, con los nuevos riesgos y retos que se derivan, supone un desafío para los auditores internos.

la seguridad de los servicios. Entre ellas, destacan:

- **Conocimientos de las distintas normativas de obligado cumplimiento, que aplican de igual modo al entorno TI en la nube:** Esquema Nacional de Seguridad (ENS), *Digital Operational Resilience Act* (DORA), *Network and Information Security* (NIS2), Reglamento general de protección de datos (RGPD), etc.
- **Conocimientos técnicos sobre las características, el funcionamiento y la seguridad de los diferentes tipos de servicios en la nube** (IaaS, PaaS, SaaS. etc.), así como sobre los distintos modelos de despliegue (privada, pública, híbrida, etc).
- **Habilidades analíticas para identificar y evaluar riesgos de seguridad** (confidencialidad, integridad, disponibilidad y autenticidad), así como los derivados de la gestión, el cumplimiento, y el gobierno de los procesos.
- **Conocimientos sobre estándares y normas internacionales** establecidas con el objetivo de proporcionar seguridad sobre la privacidad de datos personales en el contexto de servicios en la nube (ISO/IEC 27018), establecer correctamente las responsabilidades por parte tanto de la propia organización como del proveedor (ISO/IEC 27017), así como para la gestión de los riesgos (NIST SP 800-53).

Los auditores internos deben contar con una serie de competencias para aportar valor y contribuir a la calidad, eficiencia y seguridad de los servicios cloud.

Asimismo, otro aspecto a considerar serán los objetivos que se pretenden alcanzar con la auditoría de la nube, ya que las capacidades, los recursos y los tiempos pueden ser muy diferentes entre auditorías, por ejemplo, de Gobierno y Estrategia, de Configuración, de Monitorización de Actividad o de Revisión de Accesos, así como en función de quién es el auditado, si la propia organización (en adelante CSC[5], por sus siglas en inglés), o el proveedor de servicios en la nube (en adelante CSP[6], por sus siglas en inglés).

Modelos de uso e implementación de cloud

Cuando se contratan servicios en la nube se seleccionan una serie de recursos computacionales tales como servidores, sistemas de almacenamiento, aplicaciones o equipos de comunicaciones, y se dimensionan de acuerdo con las necesidades que tenga la organización (número de procesadores, memoria, capacidad de almacenamiento, número de usuarios, etc). Todos estos recursos pueden desplegarse y distribuir geográficamente entre las diferentes regiones y zonas de disponibilidad existentes, dentro de cada región que

5. *Cloud Service Client.*
6. *Cloud Service Provider.*

el CSP pone a disposición de los clientes. El precio variará según la selección y las necesidades, de tal manera que se pueda ir adaptando a lo largo del tiempo.

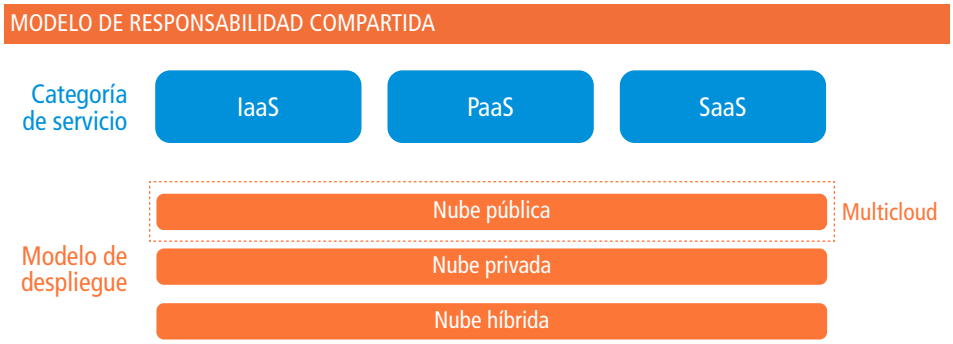
A la hora de hablar de este tipo de servicio es importante clarificar varios elementos que serán los que definan el ecosistema en la nube. Por un lado, las diversas **modalidades de servicios** en la nube se pueden clasificar atendiendo a las tipologías de servicio, entre las que se encuentran los modelos IaaS, PaaS y SaaS. Por otro lado, se deberá elegir el **modelo de despliegue o implantación,** entre los modelos de nube pública, nube privada, nube híbrida y multinube (que se refiere a utilizar más de un CSP en alguna de sus modalidades).

También es importante considerar, para los servicios a contratar, cuáles son los **mecanismos para garantizar la resiliencia y disponibilidad del servicio,** tomando en consideración tanto las zonas de disponibilidad como las regiones.

Como aspecto adicional, es relevante mencionar que, **actualmente, las compañías no optan únicamente por un modelo exclusivo de nube**, sino que distribuyen y alojan sus servicios haciendo uso de varios de los modelos mencionados (tanto de servicio, como de despliegue).

En el siguiente gráfico se ofrece una representación de cómo se relacionan los diferentes elementos que definen un servicio en la nube:

Los elementos importantes que definen el ecosistema en la nube son: modalidades de servicios, modelo de despliegue o implantación y mecanismos para garantizar la resiliencia y disponibilidad del servicio.



1. MODELO DE DESPLIEGUE O IMPLANTACIÓN

1.1. Nube privada

Una nube privada puede ser vista, en cierto modo, como el equivalente en la nube de un centro de datos corporativo; esto es, se trata de una nube que es utilizada por una sola organización.

La nube privada proporciona un control mucho mayor para las organizaciones y sus departamentos de TI. Sin embargo, también implica un mayor coste.

- VENTAJAS
  - Cumple con las políticas internas, ofreciendo mayor seguridad que la nube pública.
  - Control total de los recursos.
- INCONVENIENTES
  - Costes más elevados que en modelos de nube compartidos.
  - Dependencia de la infraestructura contratada.

1.2. Nube pública

En este modelo, los servicios y la infraestructura son proporcionados, controlados y mantenidos por el CSP a través de Internet. Con una nube pública cualquier persona que desee comprar servicios en la nube puede acceder a los recursos y utilizarlos. Los recursos son compartidos por múltiples clientes, lo que permite una mayor escalabilidad y eficiencia de costes.

- VENTAJAS
  - Escalabilidad: permitiendo aumentar las capacidades tecnológicas (resiliencia, capacidad de cómputo o almacenamiento, etc.) sin apenas esfuerzo.
  - Ahorro de tiempo y costes.
- INCONVENIENTES
  - La infraestructura es compartida, lo que para el cliente representa un reto en términos de gobierno, segmentación y aislamiento.
  - Los proveedores ofrecen poco margen de personalización del servicio al cliente.

1.3. Nube híbrida

Se trata de un entorno informático que utiliza nubes públicas y privadas en un sistema interconectado. Los usuarios pueden elegir de forma flexible qué servicios mantener en la nube pública y cuáles implementar en su infraestructura de nube privada.

- VENTAJAS
  - Maximiza el valor al utilizar recursos privados y compartidos.
  - Reduce costes respecto a soluciones tradicionales o nubes privadas.
- INCONVENIENTES
  - Riesgos al combinar dos modelos de implementación diferente.
  - Controles de seguridad en ambas nubes y en las comunicaciones entre ellas.

La siguiente tabla muestra un resumen comparativo entre los diferentes modelos de nube explicados anteriormente:

	Nubes privadas	Nubes públicas	Nubes híbridas
Flexibilidad	**Alta** (personalización del entorno).	**Media**	Combina las ventajas de ambas. Parte de los servicios se mantienen como nube privada y simultáneamente se dispone de acceso al resto de servicios de la nube pública cuando se precise. Se mantiene la seguridad, se gana en flexibilidad y se paga por lo que se usa.
Seguridad	**Alta** (recursos no compartidos).	**Media** (servicios compartidos con otros usuarios).	
Escalabilidad	**Sí** (adaptación a las necesidades del usuario).	**Sí** (adaptación a las necesidades del usuario).	
Requiere instalación HW/SW	**Sí**	**No**	
Coste	**Alto** (asociado a la adquisición y mantenimiento hardware / software).	**Medio.** Pago por servicio usado (sin mantenimiento).	
Operaciones más usuales	**Operaciones esenciales**	**Aplicaciones web** (correo, ofimática, almacenamiento, etc.)	

1.4. Multinube

Dentro de los modelos de implementación de la nube, existe un cuarto escenario, cada vez más presente en las compañías que deciden contratar servicios en la nube: el modelo multinube. En este tipo de entorno, la empresa hace uso de dos (o más) proveedores de nube pública.

En este escenario, la seguridad es esencial para el éxito de las operaciones. Por tanto, las compañías deben desarrollar una postura de seguridad sólida en entornos multinube, protegiendo los datos y recursos críticos de posibles amenazas.

Las principales ventajas y desventajas de este tipo de escenarios son las siguientes:

- VENTAJAS
  - La gestión de los recursos de la empresa es más flexible.
  - Reduce el riesgo de errores en el servidor y de pérdida de datos.
  - Uso óptimo de los servicios en línea necesarios para la empresa.
- INCONVENIENTES
  - Mayor complejidad de la infraestructura de la nube, ya que se deben gestionar más modelos diferentes
  - Posibles problemas con la transferencia de datos y la comunicación entre los diferentes CSP.

Existen cuatro escenarios dentro de los modelos de implantación en la nube: nube pública, privada, híbrida y multinube.

2. MODELOS DE SERVICIOS

2.1. Infraestructura como servicio (IaaS)

Es la categoría más flexible de servicios, ya que proporciona a una empresa la máxima cantidad de control para sus recursos. En un modelo IaaS, el CSP es el responsable de mantener el hardware, la conectividad de red y la seguridad física. El consumidor es responsable de todo lo demás: instalación, configuración y mantenimiento del sistema operativo, configuración de bases de datos y almacenamiento, configuración de red, etc.

Algunos escenarios comunes en los que IaaS podría tener sentido incluyen:

- Migración *lift-and-shift:* Consiste en poner en marcha recursos en la nube similares a los que se tienen en el centro de datos local, haciendo uso de la infraestructura de IaaS.
- **Pruebas y desarrollo:** Un entorno IaaS puede servir para establecer configuraciones en entornos de desarrollo que se necesiten replicar rápidamente. Los diferentes entornos se pueden activar y desactivar rápidamente, mientras se mantiene un control total del ecosistema.

2.2. Plataforma como servicio (PaaS)

En un entorno PaaS, el CSP mantiene la infraestructura física, la seguridad física y la conexión a Internet, así como los sistemas operativos, el middleware, las herramientas de desarrollo, etc. Un escenario PaaS proporciona un entorno de desarrollo completo, evitan-

do que la empresa sea la encargada de mantener toda la infraestructura.

Algunos ejemplos de modelo PaaS son:

- **Marco de desarrollo:** Una solución PaaS puede proporcionar un marco en el que los desarrolladores pueden basarse para desarrollar o personalizar aplicaciones utilizando componentes de software integrados, lo que reduce la cantidad de codificación que deben realizar.
- **Analítica o inteligencia empresarial:** Las herramientas proporcionadas como servicio con PaaS permiten a las organizaciones analizar y extraer sus datos, encontrar información y patrones y predecir resultados para mejorar las previsiones, rendimientos y otras decisiones empresariales.

Existen tres modelos principales de servicios: infraestructura como servicio (IaaS), plataforma como servicio (PaaS) y software como servicio (SaaS).

2.3. Software como servicio (SaaS)

Es el modelo de servicio en la nube más completo, desde el punto de vista del producto final que se ofrece. Con SaaS, básicamente se utiliza una aplicación completamente desarrollada, sin la necesidad de mantener la infraestructura y el software asociados. Si bien el modelo SaaS puede ser el menos flexible, también es el más fácil de poner en marcha. Requiere, además, del menor nivel de conocimientos técnicos o experiencia para emplearlo plenamente.

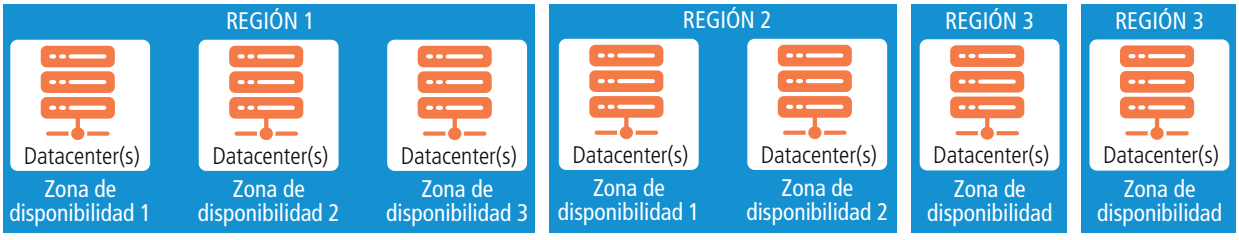
Algunos escenarios comunes para SaaS son:

- Correo electrónico y mensajería.
- Aplicaciones de productividad empresarial.
- Finanzas y seguimiento de gastos.

3. REGIONES Y ZONAS DE DISPONIBILIDAD

Otra de las ventajas de los servicios ofrecidos por un CSP, en cualquiera de sus modalidades de servicio (IaaS, PaaS o SaaS), es la posibilidad de distribuir geográficamente los recursos desplegados en diferentes ubicaciones o localizaciones físicas y/o geográficas.

En este sentido, los CSP utilizan habitualmente el concepto de "Región" para definir las localizaciones geográficas donde disponen de recursos tecnológicos. Un CSP opera en un conjunto global de regiones distribuidas por todo el mundo. Cada región del CSP está compuesta por varios centros de datos independientes, generalmente conocidos como "Zonas de disponibilidad". Las regiones están separadas físicamente entre sí y están diseñadas para ser independientes en términos de alimentación, refrigeración y redes. De esta forma se reducen los riesgos derivados de desastres naturales, interrupciones de suministro eléctrico y/o conectividades regionales. Normalmente, es habitual que los proveedores ofrezcan almacenamiento con redundancia local dentro del mismo centro de datos de la región geográfica primaria.



4. TIPOS DE REDUNDANCIA

La redundancia de datos en la nube se refiere a la práctica de almacenar copias de los datos en múltiples ubicaciones físicas, para garantizar la disponibilidad y durabilidad de la información.

Todos los CSP ofrecen varias opciones y servicios para implementar la redundancia de datos.

La redundancia, independientemente del proveedor elegido, se logra mediante la replicación de datos y servicios en múltiples ubicaciones geográficas, tanto dentro de una región como entre regiones. Los clientes pueden seleccionar las opciones de redundancia adecuadas según sus necesidades de disponibilidad, durabilidad y resistencia a fallas. Los CSP proporcionan una variedad de opciones y servicios para garantizar la integridad y la disponibilidad de los datos y los servicios en la nube. En este sentido, es responsabilidad del cliente identificar sus necesidades y riesgos para seleccionar la opción de replicación más adecuada para los servicios desplegados.

Teniendo en cuenta lo anterior, en términos generales podríamos distinguir los distintos tipos de redundancia:

- **Redundancia dentro de una región:** Dentro de una región de un CSP, los datos y servicios pueden replicarse automáticamente en múltiples zonas de disponibilidad, para garantizar la disponibilidad y la resistencia a fallas.
- **Redundancia entre regiones:** Cada CSP también suele ofrecer opciones para replicar datos y servicios entre regiones geográficas para proporcionar redundancia geográfica y mitigar los riesgos de desastres naturales o interrupciones regionales. Esto se puede lograr utilizando características como la replicación geográfica de bases de datos, el almacenamiento geo-replicado y los servicios de recuperación ante desastres.

El modelo de responsabilidad compartida establece que el CSP y el CSC comparten responsabilidades específicas por ambas partes, en cuanto a la protección de los datos, la seguridad y el mantenimiento de activos, entre otros.

Modelo de responsabilidad compartida

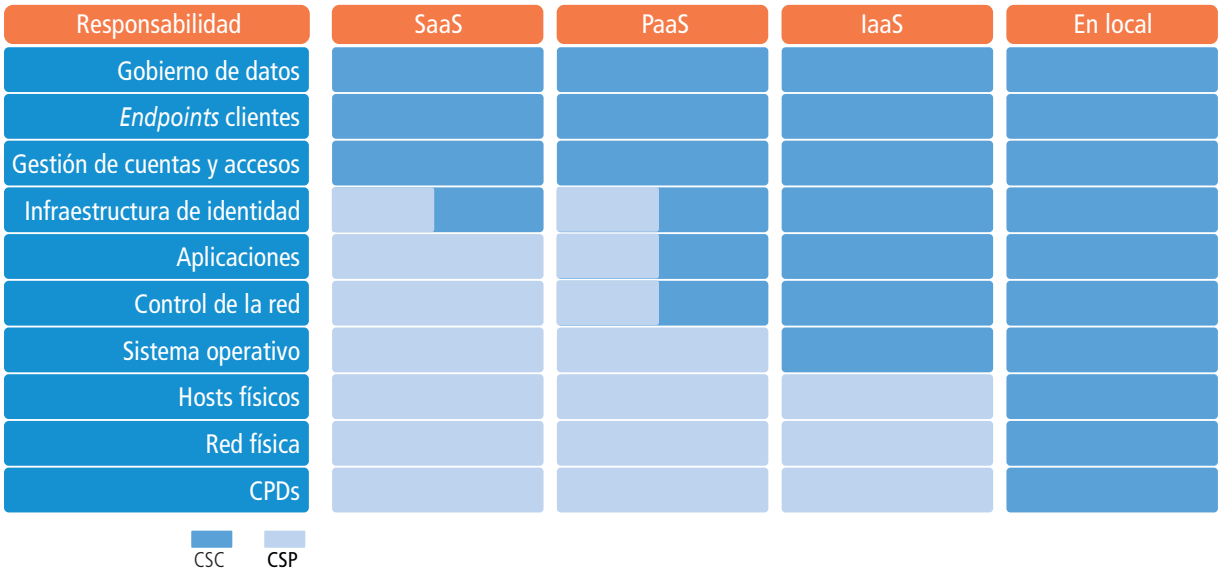
El modelo de responsabilidad compartida es un concepto fundamental en la gestión de servicios en la nube. Este modelo establece que tanto el CSP como el CSC comparten responsabilidades específicas en lo que respecta a la protección de los datos, la seguridad, el mantenimiento de activos, etc.

El modelo de responsabilidad compartida está muy ligado a los tipos de servicios en la nube IaaS, PaaS y SaaS, así como al modelo de despliegue utilizado.

Por una parte, el modelo IaaS coloca la mayor responsabilidad en el CSC y el CSP es respon-

sable de los conceptos básicos de seguridad física, conectividad, etc. En el otro extremo del espectro, SaaS coloca la mayor parte de la responsabilidad en el CSP. El modelo PaaS se encuentra en un espectro intermedio, y distribuye uniformemente la responsabilidad entre el CSP y CSC.

En el diagrama siguiente se resalta el modelo de responsabilidad compartida en función del tipo de servicio en la nube:



Con respecto a los modelos de despliegue, en la tipología de nube pública, los procesos de gobernanza en la nube se vuelven más complejos, dado que son los proveedores los responsables de su propia infraestructura. En la modalidad de nube privada, ésta puede ser gestionada tanto de manera interna como por parte de una tercera parte y, finalmente, en caso de nube híbrida, el foco deberá ponerse en alinear los SLAs y el modelo de responsabilidad compartida entre el proveedor y el establecido de manera interna, escalando la configuración de seguridad y abordando las brechas en las habilidades y la madurez en la nube.

1. MODELO DE RESPONSABILIDAD COMPARTIDA EN LOS MODELOS IaaS

En los modelos IaaS, el CSC tiene una mayor parte de responsabilidad. Dicha tipología se asemeja a los servicios de *hosting* tradicionales.

Entre los **controles que se encuentran bajo la responsabilidad del proveedor** destacan los siguientes:

- **Seguridad física de los Centros de Datos:** La seguridad física y medioambiental de los

centros de datos (control de acceso físico, cámaras de videovigilancia, sistemas de extinción de incendios, sistemas de alimentación eléctrica continua, sistemas de refrigeración, etc.).

- Mecanismos de **monitorización de consumos de CPU y memoria en los servidores**, así como de **temperatura** en las distintas salas.
- **La gestión y bastionado, tanto operativo como de seguridad, del hipervisor.** Dichos elementos permiten que múltiples sistemas operativos invitados en un solo host, asignen hardware único para ser compartido entre múltiples máquinas virtuales, lo que vincula a los proveedores de la nube a proporcionar virtualización, segmentación y aislamiento separados de componentes de la nube como CPU, GPU, sistema operativo, memoria para proteger el entorno de nube del usuario, la aplicación y los datos.
- **Mecanismos de continuidad y contingencia** que permitan garantizar la disponibilidad de la infraestructura contratada en base a los SLAs[7] establecidos con los CSC. Es habitual que los SLAs se establezcan entorno al 99,99 % de disponibilidad de servidores y demás servicios contratados.

Entre los **controles que se encuentran bajo la responsabilidad del cliente** destacan los siguientes:

- **La gestión de todas las redes virtuales** que se crean y que permiten la comunicación y segmentación entre servidores. En este sentido, es responsabilidad del CSC la implementación de dicha segmentación, así como el bastionado de dichas redes.
- **La gestión del Sistema Operativo,** incluyendo la elección del modelo y distribución a instalar, así como el mantenimiento y actualización de estos, tanto para obtener las últimas funcionalidades, como para parchear las vulnerabilidades de seguridad que vayan apareciendo.
- Todos los controles relativos a la **seguridad lógica de las aplicaciones,** desde el control de acceso lógico tanto a las propias aplicaciones, como a todo el middelware asociado (Sistema Operativo, Bases de Datos, etc), hasta el bastionado de las mismas (el aseguramiento de que no existen vulnerabilidades en el código ni en los elementos de terceros utilizados) con el objetivo de garantizar la protección de los datos almacenados.
- Controles asociados a la **gestión de copias de seguridad de los datos de las aplicaciones,** definiendo tanto los medios para dichas copias, como las periodicidades.

2. MODELO DE RESPONSABILIDAD COMPARTIDA EN LOS MODELOS PaaS

En los modelos PaaS las responsabilidades se equilibran entre el CSP y el CSC. Dicho modelo ofrece al cliente las herramientas y el entorno para desarrollar, ejecutar y gestionar sus propias aplicaciones.

7. Service Level Agreements (Acuerdos de nivel de servicio).

En este sentido, las fronteras de división de responsabilidades son menos precisas, siendo aún de mayor importancia la definición acordada entre CSP y CSC.

En este sentido, de forma general, el CSP mantiene las responsabilidades propias de los modelos IaaS, e incluye los siguientes controles:

- **El Sistema Operativo** es gestionado por el CSP, es también el responsable del mantenimiento, mediante la aplicación de parches y actualizaciones de seguridad tanto menores como mayores de los mismos.
- El CSP realiza el **aislamiento lógico de la red en la nube** y define el **control de acceso a su nube privada virtual** (VPC) junto con las operaciones de seguridad administradas. Además, facilita la definición de la segmentación de la red para admitir la arquitectura de varios niveles, así como la segregación entre múltiples redes de desarrollo, producción y corporativas.

Por su parte, el CSC mantiene la responsabilidad sobre los siguientes controles:

- La **gestión de los usuarios** tanto lógicos como genéricos o de aplicación del sistema operativo y otros middlewares utilizados y de la propia aplicación, así como el bastionado de seguridad de la aplicación.
- **La gestión de copias de seguridad.**

3. MODELO DE RESPONSABILIDAD COMPARTIDA EN LOS MODELOS SaaS

En los modelos SaaS, la balanza de la responsabilidad se decanta por el proveedor. Dicho modelo de servicio tiene retos distintos para los CSC que los modelos IaaS y PaaS, y habitualmente las organizaciones utilizan un mayor número de servicios SaaS, y habitualmente de distintos proveedores.

A su vez, es el modelo de servicio con menor control y visibilidad por parte del CSC, pero a su vez la que ofrece una mayor eficiencia y, en términos globales, menor coste.

En lo que respecta a las responsabilidades de los distintos controles, el CSP mantiene las responsabilidades asociadas a los IaaS y PaaS, y añade:

- La gestión completa de los controles asociados a los **Sistemas Operativos.**
- La gestión completa del **bastionado de seguridad de las aplicaciones.**
- La gestión de los **controles de acceso lógico a las aplicaciones.**

Bajo la responsabilidad del CSC recaen principalmente los controles asociados a la gestión de los usuarios de la aplicación, así como la protección de los datos almacenados en la misma (principalmente con la gestión de permisos de acceso de los propios usuarios a los distintos datos, así como los relativos al cifrado de estos en tránsito y en reposo).

Identificación de principales áreas responsables

Debido a que la gestión y control de la infraestructura alojada en la nube requiere la atención y participación de múltiples partes interesadas, las organizaciones suelen gestionar la estrategia y migración a la nube a través de un comité o un Centro de Excelencia en la Nube (CCOE, por sus siglas en inglés).

Para establecer las diversas responsabilidades, a menudo se utiliza una matriz de responsables, aprobadores, consultados e informados (RACI) para identificar los distintos roles y responsabilidades dentro del proceso de adopción de la nube. Ésta es utilizada para aclarar y definir los roles y responsabilidades en proyectos y procesos que involucran funciones o departamentos cruzados.

Estos roles incluidos en la matriz RACI son:

- **Responsable (R):** La persona o equipo encargado de llevar a cabo la tarea o proceso.
- **Aprobador (A):** El individuo que tiene la propiedad última de la tarea y es responsable de su éxito o fracaso.
- **Consultado (C):** Aquellos cuyos aportes se buscan, típicamente expertos en la materia, antes de tomar una decisión o acción.
- **Informado (I):** Las personas que necesitan estar al tanto de decisiones, avances o resultados, pero no están directamente involucradas en la ejecución.

La gestión y control de la infraestructura alojada en la nube requiere de la atención y participación de múltiples partes interesadas.

Aspectos de interés para Auditoría Interna

1. RETOS PARA LA FUNCIÓN DE AUDITORÍA INTERNA

El uso de plataformas y servicios en la nube supone un incremento en la complejidad de los sistemas de información de las organizaciones, así como en el tratamiento de sus datos. Este incremento de complejidad supone tanto un incremento del nivel de los riesgos ya existentes como la incorporación de nuevos riesgos inherentes al uso de este tipo de soluciones.

En este sentido, el principal reto para la Función de Auditoría Interna consiste en identificar y valorar de forma clara estos riesgos para adecuar sus planes de auditoría al uso de la

Existen múltiples desafíos a la hora de auditar servicios en la nube. Entre los más importantes, destacan: el alcance de los trabajos; la inclusión en los contratos con proveedores de cláusulas con derechos a auditarlos;múltiples ámbitos geográficos y jurisdicciones y la constante evolución de este tipo de servicios.

nube dentro de la organización, así como disponer de las habilidades y conocimientos técnicos adecuados para la realización de auditorías específicas sobre los principales riesgos.

Una vez realizado el **análisis de riesgos** sobre el entorno de sistemas de la organización, y habiendo identificado aquellos riesgos asociados al uso de plataformas en la nube tanto privadas como públicas (ya sean IaaS, PaaS o SaaS), se debe plantear un **plan de auditoría interna** que disponga de una cobertura razonable sobre los principales riesgos.

Cada iniciativa dentro del plan puede seguir un enfoque distinto para obtener un adecuado aseguramiento del entorno de control auditado. Para definir este enfoque es esencial limitar claramente el alcance de cada revisión y disponer de una comprensión clara de los entornos a auditar, así como el modelo de responsabilidades de los servicios en la nube. De este modo, se pueden distinguir dos **principales enfoques,** que pueden combinarse entre sí:

- **Auditoría del modelo interno de gestión de la nube,** para valorar las actividades de control de la propia organización sobre su ámbito de responsabilidad en dichas tecnologías, de forma análoga a las auditorías "tradicionales".
- **Auditoría del modelo de gestión del CSP,** para valorar aquellas actividades de control de este sobre su ámbito de responsabilidad (auditoría sobre terceros).

El enfoque seleccionado puede limitar la obtención de evidencias para el aseguramiento de los riesgos revisados, siendo más flexibles las revisiones sobre la propia organización que sobre un tercero, ya que los flujos de definición y obtención de evidencias pueden estar sujetos a limitaciones del tercero y pueden suponer costes adicionales, así como plazos relativamente extensos para la ejecución de la revisión.

Independientemente de la profundidad técnica de las revisiones, Auditoría Interna tiene como reto **disponer de recursos suficientemente capacitados** y con conocimiento sobre servicios y plataformas en la nube, ya sea para la realización directa de revisiones como para la coordinación y gestión de auditorías realizadas en colaboración con un proveedor especialista. Para la certificación de dichos conocimientos, existen en el mercado múltiples certificaciones y recursos para una adecuada formación de los auditores.

A continuación, se exponen los principales retos a la hora de auditar servicios en la nube:

- ALCANCE

  Al establecer el alcance de la auditoría de la nube, hay que saber qué tipo de nube y modelo de servicio se audita, ya que los requisitos de seguridad y obligaciones variarán según ello. El auditor interno debe tener un conocimiento claro de dónde comienza y termina la nube que pretende auditar.

  El alcance y los objetivos perseguidos por la auditoría deben definirse en base a un **análisis de riesgo previo**. Para dicho análisis es importante establecer una metodología de riesgos que permita identificar y evaluar aquellos riesgos más significativos de la externalización a la nube. Los riesgos de la nube pueden variar en función de la criticidad de los servicios externalizados, del grado de madurez en seguridad y privaci-

dad del CSP y la responsabilidad de ejecución de los controles entre las partes.

- **Identificación de principales *STAKEHOLDERS***

  La identificación de los principales responsables internos al ejecutar una auditoría interna sobre infraestructura en la nube presenta varios retos y complicaciones clave:

  - La gestión de la infraestructura en la nube **implica múltiples áreas** (TI, seguridad, cumplimiento, operaciones), lo que puede generar confusión sobre quién es responsable de qué. Esto es especialmente complejo cuando las responsabilidades se superponen o no están claramente definidas.
  - La seguridad en la nube puede estar distribuida entre **varios equipos,** como los de seguridad de TI, cumplimiento normativo y operaciones de red, lo que puede generar dificultades para identificar un responsable único.

  La infraestructura en la nube tiende a ser más dinámica y escalable que los entornos locales tradicionales, lo que puede generar **desafíos para identificar responsable**s de áreas específicas, ya que los servicios y configuraciones pueden cambiar rápidamente.

- **DERECHO A AUDITAR**

  Los contratos para la prestación de servicios en la nube deben contener clausulados que estipulen, siempre previa notificación, derechos de acceso, inspección y auditoría por parte de la organización cliente o de un tercero designado junto con la cooperación de este último, durante las auditorías. Este requerimiento requiere negociación con el CSP, pero cabe destacar que algunos requerimientos regulatorios y sectoriales como DORA, para el sector financiero, incluyen el derecho a auditar como uno de los requisitos de obligado cumplimiento.

- **DISPONIBILIDAD DE RECURSOS DEL CSP PARA LA EJECUCIÓN DE LA AUDITORÍA**

  Este reto es específico para aquellas auditorías que afecten al CSP. Este no dispone de recursos infinitos para atender las peticiones específicas de todos sus clientes, por lo tanto el CSP puede llegar a limitar el número de horas que dedicará a dar soporte al CSC para la ejecución de las auditorías y requerir aplazamientos y tiempos de respuesta mayores a las que estemos acostumbrados en auditorías *on-premise.*

- **LIMITACIÓN PARA PRUEBAS, REVISIONES Y RECOLECCIÓN DE EVIDENCIAS**

  El éxito de una auditoría que afecte a un CSP depende de la obtención de **evidencias suficientes y confiables.** Se tiene que tomar en consideración los siguientes aspectos en cuanto a la recolección de evidencias de auditoría:

  - Aunque el CSC tenga derecho a auditar, pueden existir reticencias, por parte del CSP, a facilitar el acceso a determinadas evidencias o ejecutar ciertas pruebas, fundamentadas en el principio de confidencialidad de la información de sus otros clientes.
  - Complejidad de los entornos en la nube: Mientras que los entornos de TI tradicionales tienen una cantidad limitada de servidores en el alcance, los componentes auditables en un entorno de nube pueden ser muy difíciles de cuantificar, ya que estos pueden variar de forma muy significativa en periodos de tiempo muy

La complejidad de los entornos en la nube supone un elemento crítico que puede suponer limitaciones para la realización de las pruebas de auditoría, revisiones y la obtención de evidencias.

Otro elemento crítico es disponer de las habilidades y conocimiento necesarios para llevar a cabo auditorías de servicios en la nube de una manera efectiva y eficiente.

cortos o ser compartidos con distintos clientes. Esto puede impactar, particularmente, en la obtención de poblaciones y muestras para la evaluación de la eficacia de los controles que se pretende auditar.

- Los entornos de nube suelen ser amplios y complejos. Es más, a medida que los proveedores desarrollan más funciones y surgen nuevas herramientas y tecnologías, el tamaño y la complejidad del entorno de la nube siguen aumentando.
- Es importante definir durante cuánto tiempo se compromete el CSP a conservar y retener los registros y eventos de auditoría.
- Es difícil la estandarización de procedimientos para la obtención, análisis y presentación de evidencias, debido a la diversidad de las arquitecturas de la nube y a que cada servicio y aplicación es distinta a las demás, debiéndose adaptar los programas y procesos de obtención de evidencias a cada caso en particular.

- **MÚLTIPLES JURISDICCIONES Y DISPERSIÓN GEOGRÁFICA**

  El uso de servicios en la nube puede suponer que la información esté dispersa en diferentes regiones y continentes, con sus propias regulaciones y legislaciones locales, lo que supone que el acceso del cliente ya no está sujeto únicamente a sus propios requerimientos internos y locales, sino que podría depender además de otras jurisdicciones. Este hecho tiene especial relevancia en los ámbitos de privacidad y seguridad.

- **CONOCIMIENTO EXPERTO**

  Otro desafío de auditar servicios y plataformas basadas en la nube es tener las habilidades y el conocimiento necesarios para realizar una auditoría de forma efectiva y eficiente. Las habilidades y el conocimiento de la nube se refieren a las competencias y la experiencia que los auditores internos necesitan para comprender las particularidades de los entornos y servicios en la nube, así como los estándares y regulaciones específicas.

  A su vez, los auditores de seguridad en la nube deben estar familiarizados con la terminología de la computación en la nube (Contenedores, hipervisores, APIs) y tener un conocimiento práctico de los servicios, controles herramientas y amenazas de un sistema en la nube. A continuación, se señalan algunos ejemplos de **certificaciones** apropiadas en términos de conocimiento sobre la seguridad en la nube:

  - CSA *Certificate of Cloud Security Knowledge* (CCSK)
  - ISC2 *Certified Cloud Security Professional* (CCSP)
  - GIAC *Cloud Security Automation* (GCSA)

- **EVOLUCIÓN CONSTANTE DE LOS SERVICIOS/AMBIENTE DE NUBE**

  Otro reto de auditar servicios y plataformas basadas en la nube es **mantenerse al día** con los cambios constantes en las mismas. La innovación es una característica intrínseca de dichos servicios, lo que conlleva a su vez, incertidumbres y potenciales nuevos riesgos para los auditores internos.

2. ROL DE AUDITORÍA INTERNA EN PROYECTOS EN LA NUBE

De forma general, podemos identificar comúnmente dos tipos de roles que Auditoría Interna puede desempeñar dentro de la compañía en relación con los proyectos en la nube.

1. Función de aseguramiento

El principal rol de Auditoría Interna, partiendo de la independencia de la función, consiste en la revisión de los entornos de control de los procesos de la organización que utilizan plataformas y servicios en la nube, haciendo hincapié en:

- **Estrategia y gobernanza de la nube:** Evaluar la estrategia de la nube para determinar si se han desarrollado políticas y controles adecuados para respaldar el enfoque de implementación general. Evaluar la alineación de la estrategia de la nube con los objetivos comerciales generales y el nivel de preparación para adoptar la estrategia dentro de la organización.

- **Seguridad y privacidad de la nube:** evaluar las prácticas y procedimientos de seguridad de la información del CSP, como informes de control de la organización de servicios (SOC), evaluaciones periódicas de seguridad y auditorías de proveedores en el sitio.

- **Revisión del servicio ofrecido por el CSP:** evaluar el servicio en la nube para determinar si se están cumpliendo los acuerdos de nivel de servicio (SLAs), a fin de cumplir con los requisitos de la organización, como disponibilidad y resiliencia, seguridad, cumplimiento, consideraciones legales y de privacidad. Evaluar planes en caso de falla o salida, cláusulas de responsabilidad, soporte extendido, disponibilidad, informes de incidentes y escalabilidad. Las funciones de Auditoría Interna también podrían determinar si el contrato de servicio en la nube aborda los requisitos de seguridad y si se han tomado medidas de seguridad internas para proteger los datos confidenciales.

2. Asesor de confianza

De forma paralela, Auditoría Interna puede actuar como asesor independiente en determinados proyectos clave de la organización relacionados con la nube: ya sea la definición de estrategias de transformación tecnológica a modelos en la nube, la adopción de nuevos servicios en la nube o la realización de proyectos, tanto tecnológicos como de negocio, apoyados en servicios en la nube, entre otros.

En este tipo de proyectos, algunos de los roles que puede llevar a cabo la función de Auditoría Interna son:

- **Asesoramiento independiente** en riesgos sobre la nube (control y gestión de riesgos en los proyectos) y Soporte en la identificación de los requerimientos no funcionales en proyectos en la nube.

- **Ayudar a la Dirección** a comprender la arquitectura de seguridad de la nube, con los riesgos y desafíos asociados.

- **Participación en los procesos de homologación** de CSPs. Auditoría interna puede ayudar a las organizaciones a diseñar procesos adecuados de selección de CSPs con

El auditor interno puede adoptar dos roles en relación con los proyectos en la nube: proveedor de aseguramiento y asesor de confianza, sin menoscabo de su independencia y objetividad.

requerimientos mínimos a tomar en consideración en la evaluación y selección de proveedores.

- **Verificación del proceso de migración** vía pruebas de calidad de datos.
- **Revisión de aspectos de control** en los modelos contractuales con CSPs (derecho de auditoría, requerimientos de control, etc.).

3. TIPOS DE AUDITORÍA EN FUNCIÓN DEL ROL DEL AUDITOR

Se pueden ejecutar diferentes tipos de auditorías en la nube según el enfoque perseguido siendo los siguientes alcances los más comunes:

- Revisión del Gobierno y del modelo de control y supervisión de servicio en la nube por parte del CSC.
- Auditoría de servicios críticos desde la perspectiva del CSC en la nube y de los controles bajo su responsabilidad.
- Revisión de los procedimientos y controles específicos ejecutados por el CSP sobre servicios prestados al CSC.
- Auditoría de migración a la nube, de manera que el CSC garantice que el traslado de la infraestructura, aplicaciones y datos se realice de manera segura, eficiente y conforme a los estándares y regulaciones aplicables.

El auditor interno tiene a su disposición diferentes herramientas de aseguramiento y tipos de revisión, para evaluar los riesgos asociados con el gobierno de la nube, la ejecución y operación de servicios en la nube y con subcontratación de servicios en la nube.

Se detallan a continuación, diferentes alternativas de tipos de revisión que pueden realizar las organizaciones para cubrir y evaluar sus riesgos en la nube con sus pros y sus contras.

TIPO	ALCANCE	DESCRIPCIÓN	VENTAJAS	DESVENTAJAS
Revisión en base a documentación pública /Certificaciones ISO/ otra documentación de interés	- Revisión CSP	- Revisión de la información general del CSP sobre el servicio ofrecido y las medidas de seguridad implementadas. - Incluye documentación pública sobre controles de seguridad y privacidad, de conformidad con estándares (ISO 27001, ISO 22301, ENS, TIER)	- La información publicada por el CSP proporciona unos datos básicos para una evaluación a alto nivel de los controles de seguridad y privacidad establecido y su cumplimiento con los requerimientos del CSC.	- La información publicada por el CSP puede no ser lo suficientemente detallada y clara para cubrir las necesidades del CSC. - La información aportada suele ser genérica, sesgada, subjetiva y favorecedora para el CSP. Esto podría llevar a una evaluación incompleta o inexacta del cumplimiento y la seguridad del CSP.

TIPO	ALCANCE	DESCRIPCIÓN	VENTAJAS	DESVENTAJAS
Ejecución de Test de intrusión por parte del CSC	- Revisión de controles gestionados por CSC - Revisión CSP	- Es una evaluación proactiva y práctica de la nube para identificar vulnerabilidades que podrían ser explotadas por atacantes. - Como CSC, se suele disponer de total libertad para ejecutar este tipo de pruebas.	- Es una forma práctica y autónoma de probar la eficacia de los controles establecidos contra los riesgos cibernéticos. - Las pruebas de penetración identifican puntos débiles de seguridad que pueden no detectarse mediante auditorías tradicionales.	- El alcance y el formato de las pruebas de intrusión pueden no estar claramente definidos. - Alcance limitado de las pruebas de intrusión y su limitación en el tiempo. El test de intrusión cubre una situación en un momento dado.
Revisión de Informes de Test de intrusión ejecutados por el CSP	- Revisión CSP	- Es una evaluación proactiva y práctica de la nube para identificar vulnerabilidades que podrían ser explotadas por atacantes. - El CSP suele realizar test de intrusiones cuyos resultados puede compartir con los CSCs.	- Es una forma práctica de evaluar la eficacia de los controles establecidos por el CSP contra los riesgos cibernéticos. - Las pruebas de penetración identifican puntos débiles de seguridad que pueden no detectarse mediante auditorías tradicionales.	- El alcance y el formato de las pruebas de intrusión pueden no estar claramente definidos. Una prueba de penetración dirigida por un CSP no es tan independiente como puede ser una prueba realizada directamente por el CSC. - Los alcances, tipos de pruebas y resultados obtenidos de los test ejecutados por el CSP pueden ser parcialmente compartido con el CSC. El CSP puede justificarlo indicando que los informes pueden contener información altamente sensible que no debe revelarse a los clientes del CSP. - Alcance limitado de las pruebas de intrusión y su limitación en el tiempo. El test de intrusión cubre una situación en un momento dado.
Revisión de Informes de Auditoría independiente sobre el CSP (informes SOC)	- Revisión CSP	- Los controles de organizaciones de servicios (SOC) son un estándar internacional desarrollado por el Instituto Americano de Contadores Públicos Certificados[8] para ayudar al CSC a evaluar los controles de seguridad que establece el CSP para garantizar la protección de información en la nube.	Los informes SOC son emitidos por una firma de auditoría independiente. Incluyen información detallada de los controles de seguridad establecidos por el CSP e información de interés para un entendimiento del entorno de Control del CSP. En concreto, incluyen: - Afirmación de la dirección: garantizar que se obtiene la confirmación de la dirección de que todos los sistemas relacionados con los	- Alcance predeterminado por el CSP por lo que puede no siempre cumplir todos los requisitos específicos del CSC. - Ciertos controles y exigencias del CSC pueden no ser cubiertos por el informe SOC. Puede que el informe no siempre contenga suficientes detalles para permitir al CSC cubrir sus riesgos de externalización al Cloud.

8. American Institute of Certified Public Accountants (AICPA).

TIPO	ALCANCE	DESCRIPCIÓN	VENTAJAS	DESVENTAJAS
		- Es un informe de auditoría independiente que evalúa, de manera imparcial y detallada, los controles operativos del CSP. - Este tipo de informe proporciona una opinión independiente sobre el diseño, implementación y la eficacia operativa de los controles establecidos por el CSP durante el período auditado (generalmente un año).	servicios prestados se describen de forma precisa y justa en el informe. - Informe del auditor incluye un resumen de todas las pruebas realizadas, así como los resultados, incluida la opinión del auditor sobre el diseño y eficacia operativa de los controles. - Visión general de los sistemas - Descripción detallada del servicio del CSP. Información muy interesante para el entendimiento de los controles establecidos.	- No hay un objetivo de "aprobado/suspenso" en los informes SOC. El resultado es una conclusión subjetiva en la que sólo consta la opinión del auditor.
Pool Audit enfocado a revisar servicios ofrecidos por el CSP	- Revisión CSP	- Una Pool Audit implica una colaboración entre un grupo de auditores de diferentes organizaciones que evalúa colectivamente los servicios del CSP. - Los CSC participan en un proceso de auditoría conjunto, compartiendo recursos y experiencia para evaluar los controles y la eficacia de un proveedor de servicios común.	- Las auditorías conjuntas permiten compartir los costes entre las organizaciones participantes, lo que reduce la carga financiera de las auditorías individuales. - Se ponen en común recursos y conocimientos especializados, las organizaciones pueden realizar auditorías más exhaustivas y alcanzar un mayor nivel de garantía.	- El alcance debe definirse con otros participantes y puede que no incluya todos los requisitos individuales. - Las pruebas aportadas en el proceso de auditoría podrían no cumplir las expectativas de cada CSC. Posibles problemas de transparencia en las pruebas aportadas.
Auditoría con alcance completo del Modelo Cloud y controles gestionados por CSC	- Modelo Cloud - Revisión controles gestionados CSC	Revisión del gobierno y modelo de control y supervisión de servicios en la nube incluyendo: - Modelo de gobierno y gestión de servicios en la nube (incluyendo roles y responsabilidades, funciones, seguimiento y *reporting* a Órganos de Gobierno, gestión de riesgos tecnológicos, entre otros). - Adecuación a la normativa y regulación aplicable al uso de plataformas en la nube. - Gestión de los Riesgos asociados al uso de in-	- Flexibilidad para determinar el alcance y el calendario de la auditoría. - Se adapta al plan de auditoría de cada CSC, al acceso a las pruebas necesarias y a los expertos en la materia. Es la Auditoría más independiente y alineada con los objetivos del CSC.	- Es la opción más compleja y costosa en recursos, tiempo y esfuerzos. Requiere conocimientos avanzados en servicios en la nube.

TIPO	ALCANCE	DESCRIPCIÓN	VENTAJAS	DESVENTAJAS
		fraestructura en la nube. - Adecuación del modelo de nube a los principales procesos tecnológicos del CSC, para dar respuesta a los riesgos específicos del uso de soluciones en la nube (seguridad de la información, operación, gestión de cambios, gestión de la continuidad). - Gestión control de los terceros involucrados en la provisión de los servicios de en la nube. En base a una metodología de priorización, se determinan los principales servicios en la nube críticos de la organización, y se realiza una revisión desde la perspectiva del CSC, tomando en consideración los controles que caen bajo su responsabilidad, y como estos son gestionados (el tipo de pruebas dependerá principalmente del modelo de servicio asociado a la nube)		
Auditoría con alcance completo de la revisión de los controles gestionados por CSP	- Revisión CSP	- La auditoría incluye la revisión exhaustiva de controles bajo la responsabilidad del CSP	- Se adapta al plan de auditoría de cada CSC, al acceso a las pruebas necesarias y a los expertos en la materia. Es la Auditoría más independiente y alineada con los objetivos del CSC.	- Es la opción más compleja y costosa en recursos, tiempo y esfuerzos, tanto internos como del CSP. Requiere conocimientos avanzados en servicios en la nube. - Las pruebas aportadas en el proceso de auditoría podrían no cumplir las expectativas del CSC. Posibles problemas de transparencia en las pruebas de revisión de CSP.

4. FUTUROS DESAFÍOS DE LA AUDITORÍA INTERNA EN PROYECTOS EN LA NUBE

El auditor interno se encuentra ante una gran cantidad de escenarios tecnológicos diferentes, a los que debe ser capaz de adaptarse.

En el apartado anterior se han descrito los retos intrínsecos que tiene Auditoría Interna en relación con los proyectos en la nube. Asimismo, es bien sabido que las infraestructuras en la nube son consideradas como una herramienta habilitadora de otras tecnologías emergentes, tales como la Inteligencia Artificial, el Blockchain, Internet de las Cosas, etc., haciendo que se abra un abanico de aspectos adicionales a considerar para las organizaciones y, a su vez, para Auditoría Interna: nuevos riesgos a identificar, regulaciones a aplicar, marcos de control a revisar, etc. Esto hace que el auditor interno se encuentre ante una gran cantidad de escenarios tecnológicos diferentes, a los que debe ser capaz de adaptarse, siendo necesario evitar el tratamiento de la infraestructura en la nube de forma aislada y, por tanto, contemplar también el servicio tecnológico de negocio que ésta pueda sustentar. Todo ello de forma conjunta, permitiendo así tener un contexto completo de cara a la auditoría. Esta situación afecta directamente tanto a los retos que han sido descritos anteriormente, como al alcance final de la auditoría o el conocimiento experto requerido por parte del propio auditor interno.

Marcos de control y de madurez específicos; estándares de seguridad y esquemas de certificación más comunes

En cuanto a normativas, esquemas de certificación, marcos de control y buenas prácticas de seguridad aplicables a los entornos en la nube, existe una extensa bibliografía; en este apartado se trata de destacar aquellas más relevantes y reconocidas en el mercado, tomándose en consideración la legislación aplicable en el marco español y europeo.

1. CERTIFICACIONES DE SEGURIDAD

1. ISO 27001

La norma ISO/IEC 27001 es reconocida a nivel mundial por establecer los **requisitos necesarios para implementar un Sistema de Gestión de Seguridad de la Información** (SGSI). Su objetivo principal es ayudar a las organizaciones a proteger la confidencialidad, integridad y disponibilidad de la información

y los activos relacionados. Esta norma proporciona un marco para gestionar los riesgos de seguridad de la información y fomenta un enfoque integral que abarca personas, políticas, procesos y tecnología. Además, incluye requisitos para la evaluación y tratamiento de riesgos de seguridad de la información, asegurando una gestión continua y efectiva.

Certificarse en esta normativa por parte de una organización indica que, para el alcance acordado, **se ha implementado un sistema para gestionar los riesgos relacionados con la seguridad de los datos y que respeta las mejores prácticas** y principios de esta norma internacional en materia de seguridad.

Cabe indicar que existen normativas relacionadas (por ejemplo, ISO27002, IS27017) que proporcionan un conjunto detallado de controles y buenas prácticas en seguridad de la información que complementan y especifican la forma en que se debe controlar y proteger la información sensible.

2. Certificación STAR

Conocida como la Certificación de la Seguridad de Proveedores de Servicios en la nube, es un programa de certificación desarrollado por el Consorcio de Seguridad en la nube *(Cloud Security Alliance,* CSA) y el Instituto de Estándares Británico *(British Standards Institute,* BSI) que ha permitido la puesta en marcha del esquema de certificación STAR, centrada en **evaluar y certificar la seguridad de los proveedores de servicios en la nube,** de manera global y confiable.

La certificación STAR tiene como objetivo proporcionar a los consumidores de servicios en la nube una forma de evaluar la seguridad de los proveedores de servicios en la nube utilizando un conjunto de criterios estándar. Estos criterios abordan aspectos como la gestión de riesgos, la seguridad de los datos, la seguridad física, la continuidad del negocio y otros aspectos relacionados con la seguridad de la información en el entorno de la nube.

Los CSP pueden someterse a una evaluación independiente de sus prácticas de seguridad utilizando el marco de la certificación STAR. Una vez que han demostrado cumplir con los estándares requeridos, reciben una certificación que pueden mostrar a sus clientes potenciales como prueba de su compromiso con la seguridad en la nube.

De esta forma, **la certificación STAR es una forma de asegurar a los usuarios que un CSP cumple con ciertos estándares de seguridad reconocidos internacionalmente.** Esto ayuda a fomentar la confianza en la nube y a promover las mejores prácticas en materia de seguridad de la información.

3. Estándar SOC2

El estándar *Service Organization Control 2* (SOC 2) ofrece un **marco de referencia para evaluar y auditar los controles de seguridad, confidencialidad, integridad, disponibilidad y privacidad de los datos en los servicios proporcionados por un proveedor de servicios en la nube.** Aunque SOC 2 no está específicamente diseñado para la auditoría exclusiva de entornos de nube, puede ser aplicado a la evaluación de la seguridad y cumplimiento en este tipo de entornos.

Dentro del ámbito de una auditoría de un CSP, el esquema de certificación SOC 2 ofrece

Las certificaciones de seguridad más conocidas son las ISO 27001; la certificación STAR y el estándar SOC2.

una estructura organizada y una metodología para la revisión de los siguientes puntos:

- Evaluación de controles de seguridad
- Confidencialidad de los datos
- Integridad de los datos
- Disponibilidad de los servicios
- Privacidad de los datos

Asociados a este esquema de certificación, existen dos tipos principales de informes SOC 2 que solo una firma acreditada puede emitir:

- **Informe Tipo I:** Este informe evalúa los controles y procesos de una organización **en un momento específico** en el tiempo.
- **Informe Tipo II:** Este informe incluye una evaluación de la efectividad operativa de los controles de una organización durante un **período de tiempo específico.** El informe Tipo II incluye una revisión más exhaustiva de los controles, evaluando su efectividad y consistencia a lo largo del tiempo.

Aunque SOC 2 **no es una certificación en sí misma,** un informe SOC 2 puede proporcionar evidencia de que una organización ha implementado controles adecuados para proteger los datos y sistemas de sus clientes. En general, un informe SOC 2 bien elaborado y emitido por una firma de auditoría independiente y puede ser una herramienta valiosa para demostrar el compromiso de una organización con la seguridad y el cumplimiento de las regulaciones en entornos de servicios en la nube. Sin embargo, es importante tener en cuenta que un informe SOC 2 **no garantiza la seguridad absoluta de una organización y sus sistemas, sino que proporciona una evaluación de los controles** implementados y su efectividad en un momento dado.

Dentro de los marcos de control y gestión de riesgos destacan especialmente la CCM de la Cloud Security Alliance; la ISO 27017; el marco del NIST y el modelo COSO de servicios en la nube.

2. MARCOS DE CONTROL Y GESTIÓN DE RIESGOS

1. CCM

La matriz de controles en la nube *(Cloud Controls Matrix* CCM[9]) está alineada con las mejores prácticas de la *Cloud Security Alliance* (CSA) y está considerada el estándar *de facto* para la seguridad y privacidad en la nube, tratando de definir un marco con los controles más relevantes en estos ámbitos, con el objetivo de ayudar a los clientes de servicios en nube a evaluar los riesgos de seguridad, independientemente del proveedor utilizado.

Actualmente está matriz (v4) cuenta con **17 dominios y 197 controles definidos.**

2. ISO 27017

La norma ISO 27017, como parte del conjunto de normas de la ISO 27001, proporciona **controles específicos sobre los servicios en la nube y define las funciones y responsabilidades de proveedores y clientes** de estos servicios, con el objetivo de que la gestión y la provisión de estos servicios aseguren la confidencialidad, integridad y disponibilidad de la información contenida. Esta normativa se centra en el despliegue, protección y separación de los activos virtualizados de los clientes, la operación y los procesos asociados de los entornos en la nube, la monitorización de la actividad de los clientes, así como la devolución y eliminación de los activos una vez finalizada la relación contractual.

3. NIST

El *National Institute of Standards and Technology* (NIST[10]) proporciona varios marcos de re-

9. Cloud Controls Matrix.

ferencia que son relevantes para entornos en la nube. Estos marcos ofrecen un conjunto de **estándares, directrices y prácticas recomendadas para identificar, mitigar y monitorizar los riesgos asociados al uso de proveedores cloud.**

También ofrecen un conjunto de estándares, directrices y prácticas recomendadas para gestionar y mejorar la **ciberseguridad,** así como un conjunto completo de controles de seguridad y recomendaciones que son ampliamente reconocidos y utilizados en la industria de la ciberseguridad.

Estos marcos de referencia del NIST son ampliamente utilizados por las organizaciones para mejorar la seguridad y la gestión de riesgos en entornos en la nube, proporcionando directrices y mejores prácticas para abordar los desafíos específicos asociados con la adopción y el uso de servicios en la nube.

3. MODELOS DE MADUREZ

1. CSMM

El modelo de madurez de seguridad en el cloud *(Cloud Security Maturity Model* - CCSM) ha sido desarrollado conjuntamente por el IANS Research y la firma Securosis y está gestionado junto con la CSA.

Su objetivo es proporcionar a los clientes una **visión del grado de madurez de la seguridad** en sus servicios en cloud, así como una hoja de ruta para su desarrollo.

Este modelo define **3 dominios con 12 categorías** que incluyen las actividades más relevantes de seguridad, y se evalúa en base a **5 niveles de madurez,** alineados con el modelo de madurez de capacidades (CMM). Cada categoría y nivel de madurez dispone de una serie de objetivos de control que se utilizan como indicadores clave de rendimiento (KPI) y para las compañías AWS, Azure y Google, adicionalmente, se disponen de ejemplos de controles de seguridad.

4. COSO sobre riesgos de los servicios cloud

El *Committee of Sponsoring Organizations of the Treadway Commission* (COSO), ha desarrollado un modelo para el gobierno y control de los riesgos asociados a los servicios en la nube[11], alineado con los marcos propios de control interno y gestión de riesgos.

Este marco proporciona una **hoja de ruta para la implementación de servicios cloud,** así como para describir de forma adecuada los **roles y responsabilidades para las organizaciones** que están en fases iniciales de dicha implementación. A su vez, para las organizaciones que ya hayan completado su migración de servicios a la nube, proporciona **mecanismos para la evaluación continua** de la misma, así como para la **mejora continua de los controles implementados** para la gestión de riesgos en este campo.

10. https://www.nist.gov/
11. Enterprise Risk Management for Cloud Computing: https://www.coso.org/_files/ugd/3059fc_96fec127be4e4f91b4ed1bdc424e73b2.pdf

4. LEGISLACIÓN APLICABLE

1. NIS2

La **Directiva (UE) 2022/2555,** conocida como NIS2, establece las medidas a aplicar con el objetivo de **garantizar un nivel adecuado y común de ciberseguridad en toda la Unión Europea,** y pretende eliminar las diferencias entre Estados miembros en la aplicación de la Directiva NIS (2016) sobre la seguridad de las redes y sistemas de información.

La Directiva NIS 2 amplía su ámbito de aplicación para abarcar a entidades medianas y grandes de más sectores críticos para la economía y la sociedad, extendiéndose a diferentes sectores divididos en 2 categorías (detalle en los Anexos I y II de la Directiva):

- **Sectores de alta criticidad** como la energía, banca, infraestructuras de mercados financieros, sector sanitario, transporte, sector espacial, aguas potables y residuales, administración pública (con excepciones), gestión de servicios TI.
- **Otros sectores** como son los CSPs, investigación, química, alimentación, servicios de mensajería, fabricación y gestión de residuos.

De forma resumida, esta Directiva establece obligaciones en la aplicación de medidas para la gestión de riesgos de ciberseguridad, obligaciones de notificación para las entidades en su ámbito de aplicación, obligaciones relativas al intercambio de información sobre ciberseguridad, así como obligaciones de supervisión y ejecución para los Estados miembros.

En primer lugar, entre las **obligaciones más destacadas a los Estados miembros** se encuentran:

- Elaborar, mantener y comunicar a la Comisión Europea un listado de entidades esenciales e importantes.
- Adoptar, notificar a la Comisión y evaluar periódicamente una estrategia nacional de ciberseguridad.
- Designar autoridades competentes de ciberseguridad, supervisión y punto de contacto único, así como notificar a la Comisión y garantizar recursos para que puedan realizar su función.
- Articular un plan nacional para gestión de crisis de ciberseguridad, así como designar autoridades competentes y determinar las capacidades necesarias.
- Designar equipos de respuesta a incidentes de seguridad informática *(Computer Security Incident Response Team* - CSIRT), así como garantizar recursos, capacidades técnicas y cooperación efectiva.

En segundo lugar, entre las **obligaciones más destacadas a las entidades** incluidas en su alcance se encuentran:

- Adoptar medidas de gobernanza, gestión de riesgos de ciberseguridad y *reporting.*
- Adoptar medidas técnicas y organizativas proporcionadas para gestionar los riesgos de ciberseguridad (destaca la inclusión de nuevos requisitos de seguridad con respecto a NIS, responsabilidad de la Dirección y la seguridad de la cadena de suministro).
- Notificación al CSIRT de referencia o a la autoridad competente cualquier incidente que tenga un impacto significativo en la prestación de sus servicios.

2. DORA

El **Reglamento (UE) 2022/2554** del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, **sobre la resiliencia operativa digital del sector financiero** (DORA[12], por sus siglas en inglés) es una iniciativa legislativa de la Unión Europea que tiene como objetivo fortalecer la resiliencia operativa digital en el sector financiero. Este reglamento es parte del paquete de finanzas digitales de la UE y es de exigible cumplimiento desde el 1 de enero de 2025.

DORA busca asegurar que las entidades financieras en la UE puedan resistir, responder y recuperarse de todas las formas de interrupciones y amenazas relacionadas con las TIC (Tecnologías de la Información y Comunicación), estableciendo un **conjunto unificado de requisitos para la gestión de riesgos de TIC en todo el sector financiero de la UE.**

DORA se aplica a una amplia gama de entidades financieras, incluyendo, entre otros, a:

- Bancos.
- Empresas de inversión.
- Proveedores de servicios de pago.
- Gestores de activos.
- Proveedores de servicios TIC críticos para el sector financiero.

Los componentes principales de este Reglamento se listan a continuación:

- **Requisitos de Gestión de Riesgos TIC**
  - Las entidades deben tener estrategias y políticas robustas para gestionar los riesgos relacionados con las TIC.
  - Se requiere la implementación de controles de seguridad y medidas de protección adecuadas.
- **Notificación de Incidentes**
  - Las entidades deben informar rápidamente a las autoridades competentes sobre cualquier incidente importante de TIC que pueda afectar la integridad, disponibilidad, continuidad y seguridad de los servicios financieros.
- **Pruebas de Resiliencia Digital**
  - Las entidades deben llevar a cabo pruebas periódicas de resiliencia operativa para evaluar la eficacia de sus estrategias de gestión de riesgos de TIC.
- **Supervisión de Terceros**
  - Se establecen requisitos específicos para la supervisión de terceros proveedores de servicios TIC, asegurando que también cumplan con los estándares de resiliencia operativa.
- **Información Compartida**
  - Promueve el intercambio de información sobre ciberamenazas y mejores prácticas entre entidades financieras.

En este sentido, cualquier proveedor de servicios cloud que albergue servicios TIC considerados críticos para una entidad financiera, deberá cumplir con los requisitos que exige el reglamento.

Por tanto, DORA es una iniciativa crucial para la modernización y protección del sector financiero en la era digital. Proporciona un **marco sólido para gestionar los riesgos asociados con las tecnologías digitales** y garantiza que las entidades financieras en la UE estén mejor preparadas para afrontar las amenazas cibernéticas y otras interrupciones operativas.

Entre la legislación que afecta a los servicios en la nube, cobran especial relevancia La Directiva NIS2; DORA; el Reglamento General de Protección de Datos; el Esquema Nacional de Seguridad y el Esquema Europeo de Certificación de Ciberseguridad en los servicios en la Nube.

12. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32022R2554

3. RGPD

El **Reglamento General de Protección de Datos**[13] (RGPD) es una legislación común de la Unión Europea que tiene como objetivo **evitar el acceso no autorizado a datos personales** y garantiza que las empresas y los individuos sepan dónde están sus datos personales, cómo acceder a ellos y cómo y cuándo se utilizan.

Las organizaciones que utilizan servicios en cloud, afrontan una serie de retos adicionales en la gestión de los datos, en un modelo de responsabilidad compartida con el proveedor de servicios, en base al tipo de servicio cloud utilizado, donde los clientes tienen el deber de garantizar que los datos personales se almacenen, procesen y transfieran de manera que cumpla con la regulación y, mientras tanto, los proveedores deben salvaguardar estos datos e implementar mecanismos de seguridad sólidos para evitar violaciones o accesos no autorizados y gestionar de forma segura la información confidencial.

Algunas de los mecanismos más relevantes se basan en un cifrado adecuado, controles de acceso a los datos, auditorías de seguridad periódicas, actualización periódica de los protocolos de seguridad, establecer procesos de autenticación sólidos y monitorizar los flujos de datos.

4. ENS

El **Esquema Nacional de Seguridad** (ENS) es una **normativa española** que tiene por objeto establecer la **política de seguridad en la utilización de medios electrónicos relacionados con la administración pública,** y está constituido por principios básicos y requisitos mínimos que permitan una protección adecuada de la información. En mayo de 2022 entró en vigor la última versión aplicable del ENS.

Este Esquema se encarga de que tanto los elementos de procesamiento y tratamiento de la información, como los sistemas de comunicación utilizados, posean la adecuada protección. **Y también afecta a los entornos de servicios en la nube.** Los proveedores de servicios en la nube que trabajen con la administración o empresas que trabajan con éstas, están obligadas a mantener la seguridad de la información, en todos los modelos de nube privada o pública, y servicios SaaS, PaaS o IaaS, y las entidades y organizaciones que trabajen con organismos públicos deben tener en cuenta las siguientes consideraciones:

- **Categorización de Sistemas.** El ENS establece un sistema de categorización de los Sistemas. La determinación de la categoría de un sistema se basa en la valoración del impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información o de los sistemas. Las entidades y organizaciones deben clasificar adecuadamente la información que manejan y aplicar las medidas de seguridad correspondientes, incluso cuando se procesa en la nube.
- **Evaluación de riesgos.** Las entidades deben realizar evaluaciones de riesgos periódicas para identificar las amenazas y vulnerabilidades que puedan afectar a la seguridad de la información en la nube. Esto in-

13. Reglamento (UE) 2016/679 del Parlamento y del Consejo, de 27 de abril de 2016, relativo a la protección de personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos (…).

cluye evaluar los riesgos específicos asociados con el uso de servicios en la nube y tomar medidas para mitigarlos.

- **Selección de proveedores.** Al elegir un proveedor de servicios en la nube, las entidades y organizaciones que trabajen con ellas deben tener en cuenta su capacidad para garantizar la seguridad de la información de acuerdo con los requisitos del ENS. Esto puede implicar la selección de proveedores que cumplan con ciertas certificaciones de seguridad o que estén sujetos a auditorías independientes
- **Contratación segura.** El ENS establece pautas para la contratación segura de servicios en la nube, considerando la inclusión de cláusulas de seguridad en los contratos con los proveedores y la verificación de que los servicios cumplen con los requisitos de seguridad establecidos por la normativa.
- **Auditoría y supervisión.** Las entidades y organizaciones que trabajen con ellas deben realizar auditorías periódicas para verificar el cumplimiento de los requisitos de seguridad en la nube y garantizar que se estén aplicando las medidas adecuadas para proteger la información.

5. EUCS

El **Esquema Europeo de Certificación de Ciberseguridad en los Servicios en la nube** (EUCS) forma parte del Esquema de Certificación de Ciberseguridad Europeo (EUCC), establece unos **estándares de ciberseguridad comunes para todos los proveedores de servicios en la nube que quieran operar en Europa,** aplicando los mismos criterios y estableciendo diferentes niveles de cumplimiento *(basic, substantial* y *high).*

Estos criterios se aplican al diseño e implementación de los servicios en nube, incluyendo sus características de seguridad y los procesos utilizados a lo largo de su ciclo de vida, en particular para el desarrollo, implementación y operación.

El esquema se compone de un **conjunto de objetivos y requisitos** de seguridad que deben cumplir los CSPs en base al nivel de cumplimiento a alcanzar, **así como unas guías que definen cómo evaluar el cumplimiento** de estos requisitos y unos procesos de evaluación específicos.

Los riesgos Cloud y cómo auditarlos

En el presente apartado se desarrolla una identificación genérica de los principales riesgos cloud al que están sujetas los CSC. A su vez, se detalla el objetivo de control que cubriría el riesgo, así como una descripción de como auditarlo, tanto en la parte cuya responsabilidad recae en el CSC, como en la parte que la responsabilidad recae en el CSP.

A continuación, se resumen los distintos riesgos que se desarrollan en las siguientes páginas:

TIPOLOGÍA DE RIESGOS	ÁMBITO DE RIESGO
7.1 RIESGOS DE ESTRATEGIA Y GOBIERNO	7.1.1 Estrategia Cloud
	7.1.2 Política y reglamentos para la nube no formalizados
	7.1.3 Mecanismos de evaluación
7.2 RIESGOS DE CUMPLIMIENTO NORMATIVO, LEGAL Y REGULATORIO	7.2.1 Riesgo de gestión del ciclo de vida de la seguridad y privacidad de los datos
	7.2.2 Riesgos de externalización de servicios en la nube
	7.2.3 Riesgo de auditoría y aseguramiento
7.3 RIESGOS OPERATIVOS Y DE CONTINUIDAD	7.3.1 Riesgo de continuidad de negocio
	7.3.2 Riesgo de gestión de cambios
	7.3.3 Adquisición, Desarrollo y mantenimiento
	7.3.4 Gestión de incidencias operativas
	7.3.5 Gestión de activos
7.4 RIESGOS DE CIBERSEGURIDAD	7.4.1 Seguridad en centros de procesamiento de datos
	7.4.2 Riesgos en criptografía, cifrado y gestión de claves
	7.4.3 Riesgo de interoperabilidad y portabilidad
	7.4.4 Seguridad en la infraestructura y virtualización
	7.4.5 Riesgos en el registro y monitorización
	7.4.6 Gestión de incidents de seguridad
	7.4.7 Gestión de vulnerabilidades
	7.4.8 Control de acceso

7.1 RIESGOS DE ESTRATEGIA Y GOBIERNO

7.1.1 ESTRATEGIA CLOUD

RIESGO: Falta de una estrategia y una hoja de ruta coherentes en la nube, o la estrategia no se encuentra alineada con las necesidades del negocio y/o la madurez tecnológica.

DESCRIPCIÓN: No disponer de una estrategia o hoja de ruta coherente para la gestión de la nube, puede derivar en que la organización no obtenga los beneficios esperados de la misma pudiendo incurrir en mayores gastos o riesgos operacionales.

OBJETIVO DE CONTROL: Objetivo de control: Se dispone de una estrategia para la nube, que se ha desarrollado considerando los beneficios previstos, la estrategia de TI de la Organización, el cambio organizacional y cualquier cambio en el modelo operativo.

CÓMO AUDITARLO

CSC

- Verificar que se dispone de documentación formal que describe la estrategia para la nube de la Organización, incluyendo objetivos clave, beneficios, cambios con respecto al modelo actual, hoja de ruta tecnológica, etc.
- Verificar que esta política/estrategia ha sido aprobadas por la alta dirección de la Organización y que se revisan de manera periódica (al menos, anualmente), incluyendo además un histórico de las aprobaciones y cambios realizados.
- Verificar que las políticas incluyen una definición formal de los roles y responsabilidades implicados en la implementación y seguimiento de la estrategia cloud, incluyendo una matriz RACI o similar.

CSP

- Evaluar, de forma cualitativa, que los CSP utilizados por la Organización dentro de su estrategia para la nube encajan con la misma.

7.1.2 POLÍTICA Y REGLAMENTOS PARA LA NUBE NO FORMALIZADOS

RIESGO: Falta de un modelo de gobierno para la gestión de la nube.

DESCRIPCIÓN: No disponer de un programa de gobierno claramente definido para la gestión del modelo en la nube (políticas, procedimientos, etc.), o que el mismo no esté alineado con las necesidades de la Organización o con su madurez tecnológica, puede derivar en que la organización no obtenga los beneficios esperados o que incurra en riesgos operacionales.

OBJETIVO DE CONTROL: Asegurar que la Organización cuenta con un programa de gobierno claramente definido para la gestión de la nube. Además, se tienen roles y responsabilidades identificados para las distintas funciones dentro del programa de gobierno. La Compañía también cuenta con un procedimiento de identificación, aprobación y revisión de excepciones al modelo GRC.

CÓMO AUDITARLO

CSC

- Verificar que se dispone de políticas y/o procedimientos definidos relacionados con el programa de gobierno de la nube, y que dispone de un adecuado circuito de revisión y aprobación.
- Verificar que las políticas incluyen una definición formal de los roles y responsabilidades implicados en la gestión y/u operación de servicios en la nube, incluyendo una matriz RACI o similar.
- Verificar que, en caso de que se tengan definidas excepciones en el modelo de gobierno, estas están claramente definidas, han sido aprobadas y existe un procedimiento de revisión periódica para estas excepciones.

CSP

- No aplica.

RIESGO: Falta de un programa de gestión de riesgos en la nube.

DESCRIPCIÓN: No disponer de un programa de gestión de riesgos derivados de la nube que incluya políticas y procedimientos para la identificación evaluación y tratamiento de los riesgos derivados de los servicios en la nube, puede derivar en que la organización incurra en riesgos por encima de su apetito al riesgo.

OBJETIVO DE CONTROL: La organización ha establecido un marco de gestión de riesgos y procesos relacionados para evaluar los riesgos derivados del servicio en la nube.

CÓMO AUDITARLO

CSC	CSP
- Verificar que la metodología para la medición del riesgo asociado a la nube está dentro de la metodología general de medición de riesgos de la Organización, así como su apetito de riesgo, y que esta tiene un adecuado circuito de revisión y aprobación. - Revisar la evaluación del riesgo realizada para los riesgos asociados a la nube, y evaluar los mecanismos utilizados para dicha evaluación (indicadores de riesgo, pruebas específicas, etc.).	- No aplica.

7.1.3 MECANISMOS DE EVALUACIÓN

RIESGO: Falta de delimitación en responsabilidades compartidas y controles complementarios de la Organización.

DESCRIPCIÓN: Una falta de determinación clara en las responsabilidades compartidas y aplicabilidad de controles dentro del marco del servicio Cloud puede resultar en asunciones indebidas y controles no ejecutados por parte del CSC.

OBJETIVO DE CONTROL: Determinar las responsabilidades claras en materia de cumplimiento y ejecución de controles a través de los dominios relevantes del servicio en la nube (Mitigación de riesgos, gestión de accesos lógicos y físicos, medidas de seguridad de red, gestión del cambio, operaciones de sistema, monitorización, etc.

CÓMO AUDITARLO

CSC	CSP
- Examinar el contrato acordado con el CSP e identificar la existencia de matrices de responsabilidades compartidas o mención a controles que debe ejecutar el CSC en su propio entorno. - Verificar la existencia de un marco formal del entorno de control propio del CSC sobre los servicios en la nube. - Evaluar el diseño y la implementación de los controles esperados en responsabilidad del CSC, incluyendo dueño de control/*accountability* asignado.	- Evaluar los mecanismos de monitorización de la efectividad de los controles gestionados por el CSP, y asegurar que entre dichos controles se encuentran todos los acordados a nivel contractual, en base a las matrices de responsabilidad compartida. - En caso de optar por una revisión del CSP basada en certificaciones, solicitar los informes asociados a la certificación SOC2 tipo 2, y verificar que entre los controles evaluados se incluyen todos los controles esperados en base a la matriz de responsabilidad compartida y que, a su vez, los controles son efectivos.

7.2 RIESGOS DE CUMPLIMIENTO NORMATIVO, LEGAL Y REGULATORIO

7.2.1 RIESGO DE GESTIÓN DEL CICLO DE VIDA DE LA SEGURIDAD Y PRIVACIDAD DE LOS DATOS

RIESGO: Falta de mecanismos de protección sobre datos sensibles.

DESCRIPCIÓN: No disponer de medidas de seguridad necesarias para proteger información confidencial, crítica o sensible almacenada, procesada o transmitida en entornos de servicios en la nube, puede implicar, en caso de pérdida del control de esta información, que la Organización tenga que afrontar riesgos reputacionales y sanciones económicas derivadas de los riesgos legales o de cumplimiento.

OBJETIVO DE CONTROL: Definir e implementar procesos, procedimientos y medidas técnicas para proteger los datos sensibles a través de su ciclo de vida.

CÓMO AUDITARLO

CSC	CSP
- Verificar que las políticas y/o procedimientos definidos relacionados con privacidad de datos, abordan los requisitos de gestión y protección de datos sensibles y confidenciales a través de todo su ciclo de vida. - Evaluar si la organización ha documentado y formalizado las funciones y responsabilidades de este proceso a través de un puesto de trabajo específico y/o área establecida (DPO, por ejemplo). - Seleccionar una muestra de datos confidenciales utilizados por el servicio en la nube desde el principio de su ciclo de vida para determinar los sistemas, procesos y controles por los cuales transita. - Identificar si se han producido filtraciones y/o violaciones de datos de la Organización e identificar las acciones realizadas a partir de las mismas.	- No aplica.

7.2.2 RIESGOS DE EXTERNALIZACIÓN DE SERVICIOS EN LA NUBE

RIESGO: Falta de definición, evaluación y monitorización de los CSP.

DESCRIPCIÓN: No disponer de un proceso de contratación de servicios en la nube puede implicar que la organización incurra en incumplimientos normativos, costos inesperados, interrupciones operativas o falta de alineación con los objetivos de negocio.

OBJETIVO DE CONTROL: Asegurar que los servicios proporcionados por proveedores externos siguen un proceso de contratación y monitorización alineado a los procedimientos de la Organización, habiendo involucrado a los distintos *stakeholders* e incorporado sus necesidades.

CÓMO AUDITARLO

CSC	CSP
- Verificar que la Organización dispone de políticas/procedimientos para compras y contrataciones. - Verificar que se ha documentado el proceso de contratación de los servicios en la nube, y que se han involucrado a todos los *stakeholders* relevantes (seguridad, cumplimiento normativo, continuidad de negocio, finanzas, etc.). - Verificar que en el proceso de contratación se ha realizado un análisis de riesgos para valorar la oportunidad de la externalización, así como los riesgos de concentración de servicios en la nube y en la dependencia de un CSP dominante. - Verificar que el contrato contiene clausulado para dar respuesta a los requerimientos de cada *stakeholder*, incluyendo aquellos relacionados con la regulación aplicable a la organización, definición de acuerdos de nivel de servicio, planes de asistencia a la terminación y cláusulas de salida (incluyendo en el contrato las obligaciones del CSP en caso de transferencia del servicio a otro proveedor de servicios o de que se reincorpore la gestión al CSC), así como los roles y responsabilidades de cada una de las partes. - Verificar que se dispone de un proceso de monitorización de los servicios en la nube, incluyendo seguimiento operativo (SLAs) y revisión de riesgos (financieros, tecnológicos, etc.). - Verificar que el CSC promueve la utilización de estándares abiertos como Kubernetes[14] y Terraform[15] para sus datos y aplicaciones en la nube.	- Comprobar que el proveedor dispone de contactos de referencia para el seguimiento del servicio. - Comprobar que el proveedor proporciona informes de seguimiento del servicio.

14. Plataforma portable y extensible de código abierto para administrar cargas de trabajo y servicios.
15. Herramienta de código abierto que permite definir los componentes de la infraestructura cloud y sus relaciones mediante un lenguaje de configuración de alto nivel.

7.2.3 RIESGO DE AUDITORÍA Y ASEGURAMIENTO

RIESGO: Ausencia de evaluaciones independientes sobre el servicio.

DESCRIPCIÓN: No realizar evaluaciones independientes de los servicios en la nube, puede implicar que los CSC incurran en riesgos de incumplimiento normativo, o en potenciales riesgos operacionales derivados ya sea de ineficiencias operativas o de incidentes operacionales.

OBJETIVO DE CONTROL: Ejecutar auditorías independientes y evaluaciones de aseguramiento, de acuerdo con las normas y/o estándares pertinentes, al menos una vez al año.

CÓMO AUDITARLO

CSC

- Examinar el proceso para determinar las normas y reglamentos aplicables a los sistemas y entornos de la organización en la nube.
- Examinar la existencia de una cláusula de auditabilidad dentro de los contratos con los CSPs.
- Determinar si la organización mantiene y revisa una lista de dichos estándares y reglamentos.

CSP

- Solicitar las renovaciones de certificaciones de seguridad (por ej. ISO27001, 27017) y auditoría de marcos ampliamente conocidos.
- Solicitar y revisar las certificaciones púbicas SOC (auditoría de terceros) que validen el diseño, implementación y eficacia operativa de los controles del CSP.
- Evaluar los resultados de los informes de auditorías externas y la necesidad de solicitar más información al CSP con respecto a los resultados particulares y que tengan afección al CSC.
- Determinar la necesidad de controles mitigantes y/o compensatorios ante cualquier problema identificado en la evaluación independiente del CSP.

RIESGO: Falta de adecuación a la normativa, regulación, legislación o requerimiento aplicable de cumplimiento.

DESCRIPCIÓN: Si un determinado servicio o proveedor en la nube contratado por un CSC no está alineado con la regulación o legislación a la que está sujeto el cliente, este va a estar expuesto a riesgos reputacionales y sanciones económicas o operativas derivadas de los riesgos legales o de cumplimiento.

OBJETIVO DE CONTROL: La organización verifica el cumplimiento de todas las normas, reglamentos, requisitos legales/contractuales y estatutarios aplicables.

CÓMO AUDITARLO

CSC

- Examinar el proceso para determinar los estándares y regulaciones aplicables a los sistemas y entornos de la Organización.
- Examinar el proceso para determinar los requisitos contractuales, legales y técnicos aplicables a los sistemas y entornos de la organización, en materia de:
  - Regulaciones por país.
  - Estándares y certificaciones aplicables.
  - Regulaciones por sector/industria.
  - Regulaciones internacionales aplicables (ej. ciberseguridad o privacidad).
- Determinar si la organización mantiene y revisa esta lista de estándares, regulaciones, requisitos legales/contractuales y estatutarios relevantes que sean aplicables al servicio en la nube.
- Determinar si el plan de auditoría está informado por la lista de requisitos de la organización.

CSP

- Evaluar el modelo de aplicabilidad del CSP y el cumplimiento de las normas que apliquen al servicio.
- En caso de optar por una revisión del CSP basada en certificaciones, solicitar los informes asociados a la certificación SOC2 tipo 2, y verificar que se han evaluado los controles vinculados al alineamiento con normativas y regulaciones de las distintas regiones de aplicación, así como que los controles son efectivos, a su vez.

7.3 RIESGOS OPERATIVOS Y DE CONTINUIDAD

7.3.1 RIESGO DE CONTINUIDAD DE NEGOCIO

RIESGO: Inadecuada gestión de la continuidad de negocio para los procesos en la nube.

DESCRIPCIÓN: No disponer de un Sistema de Gestión de la Continuidad de Negocio adecuado a los requerimientos de los servicios en la nube, y que cubra como mínimo los procesos críticos operados total o parcialmente en algún CSP, puede implicar que, ante una incidencia operacional relevante, el impacto asociado a la recuperación del servicio tenga un impacto muy relevante para la organización.

OBJETIVO DE CONTROL: Se dispone de un Sistema de Gestión de la Continuidad del Negocio, debidamente aprobado por la alta dirección, en el que se parte de un inventario de procesos, y para los que periódicamente se realiza un análisis de impacto en base a como mínimo los cuatros escenarios de disponibilidad (personas, ubicaciones, tecnología y proveedores), se identifican las dependencias y se determinan los distintos tiempos de recuperación.

CÓMO AUDITARLO

CSC

- Asegurar que el Sistema de Gestión de la Continuidad de Negocio, da cobertura a los procesos total o parcialmente externalizados en cloud, analizando que, en las dependencias de estos, se incluyen como mínimo los CSPs asociados, tomando en consideración el modelo y tipo de servicio de cloud establecido.
- Revisar las medidas establecidas en los contratos con los CSP, donde se debe establecer entre otros el RTO[16] y RPO[17] necesarios para garantizar la continuidad del servicio prestado. Así como, los planes de comunicación establecidos con las partes interesadas y los participantes en las pruebas de continuidad y resiliencia del negocio.

CSP

- Revisar las medidas contractuales establecidas.
- Solicitar los BIA[18] asociados a los servicios contratados y revisar si los mismos se ajustan a los requerimientos identificados en los propios de la Organización.
- En caso de optar por una revisión basada en certificaciones, comprobar que el proveedor dispone de certificados reconocidos y homologados (ISO22301, SOC2 tipo 2, etc.) y revisar su alcance y los resultados asociados a los controles de continuidad de negocio.

16. Recovery Time Objective: se refiere a la cantidad de tiempo que una aplicación, sistema y proceso puede estar inactivo sin causar un daño significativo a la empresa, y al tiempo dedicado a restaurar la aplicación y sus datos para reanudar las operaciones comerciales habituales después de un incidente importante.
17. Recovery Point Objective: generalmente se refiere al cálculo de cuánta pérdida de datos puede experimentar una compañía dentro de un período de mayor relevancia para sus negocios antes de que ocurra un daño significativo, desde el punto de un evento disruptivo hasta la última copia de seguridad de los datos.
18. Business Impact Analysis.

RIESGO: Inadecuado plan de pruebas para el Sistema de Gestión de la Continuidad de Negocio y la gestión de crisis.

DESCRIPCIÓN: No disponer de un plan de pruebas del correcto funcionamiento del plan de continuidad de negocio de la organización, puede implicar que, en caso de un incidente operativo, las medidas asociadas para la gestión de la continuidad no estén actualizadas y por lo tanto sean inefectivas.

OBJETIVO DE CONTROL: Se realizan pruebas periódicas calendarizadas y documentadas del Plan de Continuidad de Negocio, en base a las escenarios y estrategias definidos, contemplando, como mínimo, los 4 escenarios de indisponibilidad (personas, ubicaciones, tecnología y proveedores).Además, se pone en práctica el plan de respuesta ante desastres anualmente, o ante cambios significativos, incluidos todos los actores involucrados (comité de crisis, alta dirección, áreas técnicas y de negocio, etc.).

CÓMO AUDITARLO

CSC

- Validar que, en el Sistema de Gestión de la Continuidad de Negocio, se consideran las pruebas a realizar en función de los servicios en la nube asociados a los procesos que deben ser probados. A su vez, verificar que se realizan pruebas que den cobertura a los distintos escenarios de indisponibilidad.
- En las pruebas, considerar en función de los servicios, los siguientes aspectos:
  - En los servicios IaaS, identificar la estrategia de recuperación implementada, y evaluar si en las pruebas efectuadas de la misma, se permite cubrir los RTO y RPO previstos.
  - En los servicios PaaS, hay que asegurar que el plan de respuesta permite cubrir con los RTOs y RPOs.
  - En los servicios SaaS, asegurar que el CSP dispone de pruebas de recuperación que se ajustan a los requerimientos de tiempos de recuperación de la organización.

CSP

- Revisar el calendario de pruebas y los informes de estas, garantizando que se han considerado como mínimo: personal involucrado, activos, fases de ejecución medición de tiempos, documentación utilizada, cumplimiento de RTOs y lecciones aprendidas.
- Comprobar que se dispone de un plan de gestión de crisis, dónde se establezcan los roles y responsabilidades, para una adecuada comunicación y ejecución de los pasos a seguir.

7.3.2 RIESGO DE GESTIÓN DE CAMBIOS

RIESGO: Paradas o errores imprevistos en los procesos de cambios y mantenimiento.

DESCRIPCIÓN: Errores en los cambios (código defectuoso, cambios en configuraciones que llevan a errores, colisión de cambios, etc.) que dan pie a una operación defectuosa sin intención por parte del usuario, pero con consecuencias sobre la integridad de los datos o la disponibilidad del servicio.

OBJETIVO DE CONTROL: Existe un proceso de gestión de cambios con responsabilidades claras de las partes para garantizar que los cambios que impactan al CSC se planifican, revisan, prueban, aprueban y comunican adecuadamente.

CÓMO AUDITARLO

CSC

- Asegurar que todos los cambios producidos en el servicio en la nube son gestionados siguiendo el proceso de cambios de la Organización, de forma que los cambios en servicios en la nube sean registrados, autorizados, probados, desplegados y documentados. Respecto a las pruebas, el CSC y el CSP deben acordar de antemano la responsabilidad y el alcance de las pruebas a realizar.
- Comprobar que se evalúa el impacto y potenciales riesgos asociados al cambio propuesto previo a su implementación
- Verificar que el acuerdo con el CSP define los procesos, triggers y canales de notificación de cambios a programa, por parte del CSP al CSC. Comprobar que están definidos y establecidos qué tipo de cambios no requieren ser informados al CSC.

Particularmente en un SaaS:

- Identificar si los cambios notificados por el proveedor son registrados en la herramienta de gestión de cambios de la Organización.
- Verificar que el acuerdo con el CSP define los procesos, *triggers* y canales de notificación de cambios a programa, por parte del CSP al CSC. Comprobar que están definidos y establecidos qué tipo de cambios no requieren ser informados al CSC.

CSP

- Verificar que el CSP dispone de un procedimiento sistemático para gestionar los cambios y garantizar que todos los cambios en entorno productivos son revisados, testeados y aprobados.
- Validar que el enfoque de gestión de cambios del CSP requiere que se completen los siguientes pasos antes de implementar un cambio en el entorno de producción:
  - Registrar y Documentar el cambio a través de la herramienta de gestión de cambios.
  - Planificar la implementación de los procedimientos de cambio y reversión para minimizar las interrupciones.
  - Probar el cambio en un entorno no productivo, segregado lógicamente del entorno productivo. La revisión debe incluir una revisión del código.
  - Establecer un proceso que permite retroceder hasta el anterior estado correcto conocido en caso de error o problema en el cambio.
  - Comprobar que existe una comunicación clara entre el CSP y el CSC para anuncios de cualquier aspecto, incluidos cambios que puedan afectar la continuidad de los servicios de sus clientes.

RIESGO: Errores de configuración.

DESCRIPCIÓN: Disponer de activos tecnológicos con errores de configuración tales como cuentas y contraseñas predeterminadas, permisos excesivos a usuarios, almacenamiento de datos sin cifrar o falta de actualizaciones, puede derivar en riesgos de seguridad o en riesgos operativos que puedan impactar en la confidencialidad, integridad y disponibilidad de la información y los servicios.

OBJETIVO DE CONTROL: Reducir la superficie de ciberataque sobre los componentes en la nube, a través de bastionado.

CÓMO AUDITARLO

CSC

Únicamente de aplicación en IaaS y PaaS:

- Verificar que el CSC dispone de documentación completa de bastionado para cada tipo de sistema y distribución e incluye detalles de la configuración base de seguridad y listas de comprobaciones de seguridad de la configuración de las instancias.
- Evaluar el proceso de homologación y validación de las configuraciones base de seguridad de los componentes en la nube, por parte del CSC sobre las imágenes base ofrecidas por el CSP. Validar que las imágenes por defecto de las máquinas virtuales ofrecidas por el CSP se comparan respecto a las prácticas autorizadas por el CSC u otros estándares reconocidos de mercado como CIS Benchmark o NIST.
- Comprobar que el CSC dispone de controles y herramientas de monitorización de las configuraciones de los componentes de la nube y se detectan todas las desviaciones respecto a la configuración base. En caso de identificar discrepancias, los detalles se documentan y se devuelven al equipo responsable para su corrección.
- Verificar que se dispone de un repositorio de configuraciones base con un historial de todos los cambios, así como la última configuración actual facilitando de este modo cualquier proceso de rollback a una configuración operativa.
- Verificar que sólo las personas autorizadas pueden obtener acceso a los componentes del sistema de información con el fin de iniciar cambios en las configuraciones. Verificar que se dispone de un proceso de recertificación de usuarios privilegiados.

CSP

- Verificar que los procesos de gestión de configuración del CSP cubre las configuraciones básicas, control de cambios de configuración, la supervisión de cambios de configuración, el establecimiento de ajustes de configuración y la aplicación del principio de mínimo privilegio.
- Asegurar que las instancias puestas a disposición de los CSC han pasado por un proceso de registro, aprobación, testing y validaciones internas.
- Verificar que el CSP lleva a cabo un proceso de revisión continua de sus configuraciones base, respecto a los estándares de seguridad en la nube de la industria.
- Comprobar que el CSP pone a disposición del CSC herramientas que permitan al CSC auditar y evaluar continuamente las configuraciones y relaciones de sus recursos en la nube.

7.3.3 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO

RIESGO: Inadecuado ciclo de vida del desarrollo en la nube.

DESCRIPCIÓN: Alteración intencionada o accidental del funcionamiento de los programas que dan pie a una operación defectuosa con consecuencias sobre la integridad de los datos o la capacidad misma de operar.

OBJETIVO DE CONTROL: Garantizar que la seguridad de la información sea parte integral de los sistemas de información en la nube, a través de todo su ciclo de vida de desarrollo.

CÓMO AUDITARLO

CSC

- Verificar que el CSC dispone de un procedimiento de seguridad en proyectos en la nube que asegura que:
  - La adquisición, desarrollo y gestión de servicios en la nube incorpora requisitos de privacidad y seguridad tecnológica.

CSP

- Verificar que el CSP dispone de una política de desarrollo seguro que cubre los siguientes aspectos:
  - Proceso de desarrollo seguro para software, aplicaciones y servicios desarrollados por el CSP.
  - Requisitos de revisión y certificación de seguridad antes de que un software desarrollado por el CSP pueda promocionarse a un entorno de producción.
  - Requisitos de nivel de servicio, incluido el seguimiento del flujo de datos.

CÓMO AUDITARLO

· Se definen los roles y responsabilidades en el ámbito de la privacidad y la seguridad tecnológica en la gestión de proyectos en la nube.
· Se definen requisitos de seguridad a cumplir en función del uso previsto del desarrollo en la nube
· Se valida la implementación de los requisitos de seguridad definidos en la fase de diseño del proyecto de externalización en la nube.

- Verificar que el acuerdo con el CSP define los roles y responsabilidades de las partes sobre los diferentes entornos en la nube (desarrollo, test, calidad, preproducción, producción, etc.)

· Limitaciones en el acceso a datos de producción.
· Mantener actualizado el software de producción del CSP con los últimos parches de seguridad.

- Asegurar que el ciclo de vida de desarrollo del CSP cumple con las mejores prácticas de la industria (Guía OWASP, CERT Secure Coding. etc.) en cuanto a:
· Gestión de autenticación y contraseñas.
· Administración de sesiones.
· En el software desarrollado solo se utilizan algoritmos de cifrado estandarizados.
· Protección del sistema operativo del *host*.
· Gestión de errores y *logs*.
· Seguridad en las comunicaciones.
· Seguridad de base de datos.
· Gestión de archivos y seguridad en el almacenamiento.
· Gestión de memoria.
· Protección de contenedores.
· Seguridad en los procesos de *DevOps*.

RIESGO: Acceso no autorizado al código fuente.

DESCRIPCIÓN: El acceso no autorizado al código fuente puede derivar en riesgos de seguridad tales como la explotación de vulnerabilidades, la inyección de malware o la interrupción del servicio.

OBJETIVO DE CONTROL: Determinar el nivel de seguridad del Código fuente e identificar todos los puntos de acceso y brechas que podrían producirse para una aplicación en particular.

CÓMO AUDITARLO

CSC

- Verificar que el CSC dispone de un repositorio de código fuente de sus aplicaciones en la nube que cubre las siguientes medidas de seguridad:
· Acceso restringido al repositorio con diferentes roles definidos. Los roles son asignados por aplicación/servicio/proyecto, por lo que el acceso se encuentra limitado a los elementos asignados.
· Se respeta la segregación de funciones en los accesos a la fuente. Los desarrolladores no puedan aprobar el pase a producción de los cambios que han desarrollado.
· Los programas fuente no se guardan en los sistemas de producción.
- Comprobar que existen controles implementados en el sistema de repositorio de código para dejar trazabilidad de todas y cada una de las modificaciones y cambios realizados.

CSP

- Revisar que el CSP tiene inventariado todos los repositorios de código fuente y mantiene un control seguro sobre todos ellos. Se aplican medidas de seguridad para que únicamente personal autorizado pueda acceder a ellos según sea necesario.
- Verificar que el CSP mantiene un registro de auditoría para todos los accesos a las fuentes.
- Asegurar que el mantenimiento y las copias de seguridad de las fuentes están sujetas a procedimientos de control de cambio estrictos.
- Comprobar que el CSP almacena el código, los archivos binarios y los metadatos de una forma redundante y con alta disponibilidad.
- Verificar si el CSP implementa software de código abierto dentro de sus servicios y comprobar los controles de revisión y aprobación establecidos para su uso adecuado.

RIESGO: Accesos a datos del CSC en entornos no productivos.

DESCRIPCIÓN: Los datos de clientes pueden llegar al conocimiento de personas que no deberían tener conocimiento de ellos, sin que la información en sí misma se vea alterada, pudiendo derivar en que la Organización tenga que afrontar riesgos reputacionales y sanciones económicas derivadas de los riesgos legales o de cumplimiento.

OBJETIVO DE CONTROL: Evitar el uso de datos de producción del CSC en entornos no productivos para la ejecución de pruebas.

CÓMO AUDITARLO

CSC

- Verificar que los entornos productivos y no productivos están lógicamente separados vía revisiones de reglas de tráfico y otras pruebas de penetración.
- Verificar que el CSC mantiene el código y los datos alojados en un espacio privado a la que solo podrán acceder quienes sean parte de esa red. Verificar las restricciones de todo el tráfico entrante a los entornos de desarrollo, los repositorios de código, en particular el tráfico desde Internet.
- Realizar pruebas para verificar que no existen datos de producción en entornos no productivos.
- Si estos se localizan, verificar que, son adecuadamente eliminados.

CSP

- Comprobar que el CSP tiene establecidos controles de acceso independientes para entornos productivos y no productivos.
- Verificar los controles establecidos por el CSP para garantizar que las herramientas de desarrollo no son accesibles desde los sistemas productivos.
- Comprobar que el CSP revisa periódicamente los accesos de usuarios de desarrollo.

7.3.4 GESTIÓN DE INCIDENCIAS OPERATIVAS

RIESGO: Inadecuada gestión de incidencias asociadas a servicios en la nube.

DESCRIPCIÓN: Una inadecuada gestión de incidencias en un servicio en la nube puede provocar interrupciones de servicio, degradaciones o pérdidas de datos, afectando negativamente a la continuidad del negocio, a la satisfacción de los clientes o al cumplimiento de SLAs, así como tener otros impactos de índole financiero, legal y reputacional.

OBJETIVO DE CONTROL: Se dispone de un adecuado marco de gobierno que define los pasos a seguir y los roles y responsabilidades necesarios para una adecuada gestión de las incidencias que afecten a los servicios en la nube, así como para que se restablezca el funcionamiento normal de los servicios lo antes posible, minimizando el impacto negativo sobre los clientes y la calidad del servicio.

CÓMO AUDITARLO

CSC

- Comprobar que el marco de gobierno y los procesos de gestión de incidencias internos incluyen las incidencias asociadas a los componentes en la nube en función del tipo de servicio, habiendo definido los roles y responsabilidades necesarios para una adecuada gestión de incidencias.
- Verificar que se realiza una clasificación y seguimiento de las incidencias en base a la criticidad de éstas y que se monitoriza el cumplimiento de los tiempos de resolución.

CSP

- Comprobar las referencias en los informes SOC2 tipo 2 del proveedor sobre cómo se comunican y gestionan las incidencias en su infraestructura o servicios, para poder evaluar su cumplimiento y analizar los SLAs establecidos a nivel contractual.

7.3.5 GESTIÓN DE ACTIVOS

RIESGO: Desconocimiento del parque tecnológico.

DESCRIPCIÓN: No disponer de procesos adecuados para mantener un inventario completo de activos tecnológicos puede derivar, entre otros, en errores de configuración o en políticas de seguridad ineficaces.

OBJETIVO DE CONTROL: Se dispone de procedimientos formalizados en los que se define como gestionar las altas, bajas y modificaciones de todos los activos tecnológicos, poniendo especial foco en todos aquellos desplegados en modalidad en la nube.

Todos los controles asociados a estos procedimientos deberán asegurar de manera razonable la completitud y exactitud de la información almacenada en los inventarios TIC.

CÓMO AUDITARLO

CSC

- Identificar que los procesos de gestión de activos tecnológicos en relación con altas, bajas y que aseguran la completitud y la exactitud de los inventarios. Los controles derivados de estos procesos deben de poner foco en los activos tecnológicos de tipo IaaS (en el inventario de infraestructura), PaaS (complementando la información de la propia infraestructura con la relativa a Bases de Datos, Sistemas Operativos, almacenamiento, etc.) y SaaS (centrado en elementos software/aplicaciones del inventario) desplegados en cualquier tipo de modalidad cloud.

CSP

- Identificar y revisar los inventarios tecnológicos, así como los controles para el descubrimiento de los activos creados.
- En caso de optar por una revisión del CSP basada en certificaciones, solicitar los informes asociados a la certificación SOC2 tipo 2, y verificar los controles vinculados a la gestión de inventarios de infraestructura, de elementos tecnológicos vinculados a los servicios IaaS, PaaS, así como a los servicios SaaS.

RIESGO: Inventarios con información no actualizada.

DESCRIPCIÓN: No disponer de procesos adecuados para mantener la información de todos los activos tecnológicos adecuadamente registrada y actualizada puede derivar, entre otros, en errores de configuración o en políticas de seguridad ineficaces.

OBJETIVO DE CONTROL: Toda la información considerada relevante asociada a un activo tecnológico está convenientemente registrada y se actualiza adecuadamente en un periodo razonable.

Se dispone de controles para asegurar que toda la información es registrada y actualizada correctamente.

CÓMO AUDITARLO

CSC

- Identificar que los procesos de gestión de activos tecnológicos en relación con el mantenimiento y que aseguran la completitud y la exactitud de los inventarios. Los controles derivados de estos procesos deben de poner foco en los activos tecnológicos de tipo IaaS (en el inventario de infraestructura), PaaS (complementando la información de la propia infraestructura con la relativa a Bases de Datos, Sistemas Operativos, almacenamiento, etc.) y SaaS (centrado en elementos software/aplicaciones del inventario) desplegados en cualquier tipo de modalidad cloud.

CSP

- Identificar y revisar los inventarios tecnológicos, así como los controles para el mantenimiento de los activos de este.
- En caso de optar por una revisión del CSP basada en certificaciones, solicitar los informes asociados a la certificación SOC2 tipo 2, y verificar los controles vinculados a la gestión de inventarios de infraestructura, de elementos tecnológicos vinculados a los servicios IaaS, PaaS, así como a los servicios SaaS.

7.4 RIESGOS DE CIBERSEGURIDAD

7.4.1 SEGURIDAD EN CENTROS DE PROCESAMIENTO DE DATOS

RIESGO: Desastre natural /industrial.

DESCRIPCIÓN: Los incendios, cortes de suministro eléctrico, inundaciones o desastres naturales pueden causar daños irreparables en los equipos de los Data Centers e impactar en la continuidad del negocio.

OBJETIVO DE CONTROL: Existen mecanismos para minimizar el efecto de un mal funcionamiento o desastre en las instalaciones del centro de datos.

CÓMO AUDITARLO

CSC

- Verificar que el CSC solicita al CSP informes de acreditación de Seguridad de los CPDs[19] realizada por entidades externas (SOC 2, Informe de certificación TIER) que evalúan las medidas medioambientales establecidas.

CSP

- Verificar que los centros de Datos del CSP disponen de medidas medioambientales adecuadas para el eficaz funcionamiento del equipamiento allí instalado y, en especial, para asegurar:
  - Las condiciones de temperatura y humedad.
  - La protección del cableado frente a incidentes fortuitos o deliberados.
  - El abastecimiento eléctrico de contingencia, en caso de fallo del suministro principal.
  - Medidas de protección frente a incendios e inundaciones.
- Comprobar que, para la elección de los emplazamientos de los centros de Datos, el CSP ha realizado evaluaciones medioambientales y geográficas para mitigar los riesgos medioambientales, como inundaciones, condiciones climáticas extremas y actividad sísmica. Verificar que el CSP realiza revisiones periódicas de amenazas y vulnerabilidades de los centros de datos. La evaluación y mitigación continuas de las posibles vulnerabilidades se realizan a través de actividades de evaluación de riesgos del centro de datos.

ASPECTOS QUE CONSIDERAR: Los Centros de Datos del CSP pueden ser subcontratados parcialmente, o en su totalidad, a empresas de servicios de colocación. El CSC tiene que asegurarse de que el CSP tenga contratos en vigor con sus empresas de servicio de colocación y que éstas aplican las mismas medidas de seguridad física y medioambiental que el CSP aplica a sus propios centros de Datos. El CSC tiene también que validar qué revisiones y comprobaciones realiza el CSP a sus servicios de colocación para validar el cumplimiento de los requisitos de seguridad física y medioambiental.

19. Centros de Procesamiento de Datos.

RIESGO: Acceso físico no autorizado.

DESCRIPCIÓN: Cualquier individuo con acceso físico a los centros de datos puede introducir dispositivos y acceder a los recursos sin la debida autorización. Esto puede incluir visitantes, contratistas o incluso empleados maliciosos que pueden aprovechar esta vulnerabilidad para robar datos, instalar *malware*, realizar actividades de vandalismo perjudiciales para la organización.

OBJETIVO DE CONTROL: El acceso físico a los centros de datos está restringido a personas autorizadas.

CÓMO AUDITARLO

CSC

- Verificar que el CSC solicita al CSP informes de acreditación de Seguridad de los CPDs realizada por entidades externas (SOC 2, Informe

CSP

- Verificar que el acceso físico a los centros de datos del CSP es aprobado por personal autorizado. Estas solicitudes se deben conceder en función del principio de privilegios mínimos, según el cual las solicitudes deben especificar a qué capa del centro de datos requiere acceso la persona, con limitaciones temporales.
- Comprobar que el acceso a la sala de servidores se hace a través de dispositivos electrónicos de control de acceso y que se registran los accesos de entrada y salida a las salas de servidores del CSP dónde se

	de certificación TIER) que evalúan las medidas medioambientales establecidas.	ubican los componentes que soportan la actividad del CSC. El acceso físico a los centros de datos del CSP se monitoriza y se mantiene a través de procesos de recertificación de usuarios con acceso a los centros de datos. El CSP correlaciona la información obtenida de los sistemas de monitorización lógicos y físicos para mejorar la seguridad según sea necesario. Verificar también los controles de acceso de seguridad perimetral y que los puntos de acceso físico a las salas de servidores se graban con cámaras de televisión de circuito cerrado (CCTV). Las imágenes se conservan de acuerdo con los requisitos legales y de conformidad. - Comprobar que el CSP dispone de controles de entrada y salida de equipamiento a las instalaciones. Comprobar que se lleva un registro de cualquier entrada y salida de equipamiento, incluyendo la identificación de la persona que autoriza el movimiento. - Validar que el CSP dispone de un procedimiento de decomisionado de activos de información asegurando que ningún activo con información del CSC salga de las instalaciones del CSP.

7.4.2 RIESGOS EN CRIPTOGRAFÍA, CIFRADO Y GESTIÓN DE CLAVES

RIESGO: Existencia de vulnerabilidades en algoritmos criptográficos o en su implementación y configuración en los sistemas del CSP o en el CSC.

DESCRIPCIÓN: No se utilizan algoritmos y/o implementaciones criptográficas seguras y correctas, pudiendo exponer los datos cifrados a riesgos adicionales.

OBJETIVO DE CONTROL: Se dispone de políticas y procedimientos que establecen los criterios de los algoritmos criptográficos que deben ser utilizados. A su vez, únicamente se utilizan algoritmos criptográficos seguros, y para los que no se les conocen vulnerabilidades.

CÓMO AUDITARLO	CSC	CSP
	- Revisar la existencia de políticas y procedimientos respecto a la gestión criptográfica del CSC (desde los requerimientos de comunicación y almacenado, hasta criterios más operativos o de implementación). - Asegurar que todas las comunicaciones con los CSPs se realizan siguiendo los criterios establecidos en las políticas y procedimientos.	- Verificar que se realiza una correcta gestión de métodos y algoritmos criptográficos que permiten utilizar, y que únicamente se permiten aquellos que no contengan vulnerabilidades que podrían ser explotadas por atacantes para descifrar la información contenida en ellos, así como su correcta implementación y configuración sin que contengan errores que puedan ser aprovechados por atacantes.

RIESGO: Generación, gestión, rotación y destrucción no adecuada de claves criptográficas por parte del CSC.

DESCRIPCIÓN: Una inadecuada gestión de claves, como el almacenamiento inseguro o la falta de rotación de claves, puede exponer los datos cifrados a riesgos adicionales.

OBJETIVO DE CONTROL: Existen políticas y procedimientos formalizados que aseguren una correcta generación, gestión, rotación y destrucción de las claves criptográficas utilizadas, así como procesos de auditoría y revisión de su correcta implementación, comprobando específicamente la aleatoriedad en la generación de estas.

CÓMO AUDITARLO	CSC	CSP
	- En caso de que, para los servicios en la nube, sea el propio CSC quien sea el responsable de las claves criptográficas, asegurar que existen políticas y procedimientos formalizados y adecuados para la gestión de claves que gestionen la generación, registro, almacenamiento, distribución, uso, rotación y revocación de estas de manera	- Asegurar que existen políticas y procedimientos formalizados y adecuados para la gestión de claves que gestionen la generación, registro, almacenamiento, distribución, uso, rotación y revocación de estas de manera segura. Asimismo, se deberá comprobar la existencia periódica de

	segura. Asimismo, se deberá comprobar la existencia periódica de auditoría de los sistemas involucrados en toda la gestión de las claves criptográficas, y tras cualquier incidente que se pueda producir.	auditoría de los sistemas involucrados en toda la gestión de las claves criptográficas, y tras cualquier incidente que se pueda producir.

7.4.3 RIESGO DE INTEROPERABILIDAD Y PORTABILIDAD

RIESGO: Riesgos de seguridad de la información debidos a la interoperabilidad entre múltiples nubes.

DESCRIPCIÓN: Las capacidades de interoperabilidad entre múltiples nubes añaden complejidad al entorno de seguridad *end-to-end,* incrementando los riesgos de gestión, intercambio, retención y eliminación de la información y los datos entre las plataformas.

OBJETIVO DE CONTROL: Se dispone de un marco de gestión de entornos *multinube* de manera que se asegura una adecuada aplicación de los controles de ciberseguridad en las diferentes nubes, en especial los relacionados con la gestión e intercambio de información.

CÓMO AUDITARLO	CSC	CSP
	- Identificar y evaluar los procesos de interoperabilidad entre nubes, incluyendo aspectos de comunicación entre las plataformas, procesamiento de la información, portabilidad de las aplicaciones, /uso/intercambio/persistencia de la información y los datos. - Identificar la existencia de herramientas/plataformas CMP para la gestión de entornos multinube. En caso de existir, evaluar el alcance de estas y los mecanismos utilizados para garantizar una aplicación de los controles de seguridad en las diferentes nubes, especialmente los relacionados con la gestión e intercambio de la información (encriptación en reposo y tránsito, retención, eliminación, etc.). - En su defecto, identificar y evaluar los procesos de ciberseguridad y su aplicación en las diferentes nubes, especialmente los relacionados con la gestión e intercambio de la información (encriptación en reposo y tránsito, retención, eliminación, etc.).	- Evaluar la existencia y disponibilidad de aplicaciones al servicio de los CSCs para permitir la interoperabilidad y portabilidad. - Comprobar en el SOC2 tipo 2 de los CSP, los resultados asociados a los controles de gestión de la seguridad asociados, específicamente los relacionados con la gestión e intercambio de información (encriptación en reposo y tránsito).

RIESGO: Riesgos de continuidad en los servicios en la nube debidos a la falta de mecanismos de portabilidad a otros entornos.

DESCRIPCIÓN: Ante un evento disruptivo que comprometa la continuidad de un entorno en la nube (discontinuidad de un proveedor, no renovación contractual, interrupción de operaciones, etc.), carencia de las capacidades para trasladar los datos, aplicaciones y servicios a un proveedor alternativo y/o al entorno *on-premise* del cliente, de manera que se asegure una adecuada continuidad de los servicios afectados.

OBJETIVO DE CONTROL: Evaluar los procedimientos, interfaces y mecanismos para la migración de los datos y aplicaciones a otro entorno alternativo (nube u *on-premise)* de manera que se asegure una adecuada continuidad de los servicios afectados.

CÓMO AUDITARLO	CSC	CSP
	- Identificar la existencia de una estrategia de "cloud neutral", así como los estándares utilizados para asegurar una dependencia limitada con el CSP, así como los interfaces y mecanismos de migración a un entorno alternativo. - Identificar los procedimientos de recuperación y puesta en marcha de los servicios en la nube, y evaluar la existencia de escenarios que afecten a la continuidad del proveedor ante un evento disruptivo. - En caso de estar el escenario identificado, evaluar la existencia de pruebas periódicas de recuperación ante desastres, para la migración y puesta en marcha de los datos, aplicaciones y servicios al entorno alternativo.	- No aplica.

7.4.4 SEGURIDAD EN LA INFRAESTRUCTURA Y VIRTUALIZACIÓN

RIESGO: Falta de integridad en imágenes de máquinas virtuales/contenedores.

DESCRIPCIÓN: Despliegue de imágenes de máquinas virtuales/contenedores con fallas de integridad debido a la realización de modificaciones no autorizadas o maliciosas, pudiendo derivar en accesos no autorizados, fugas de datos, fallos en el hardware y otras vulnerabilidades.

OBJETIVO DE CONTROL: Cualquier cambio realizado en las imágenes de las máquinas virtuales/contenedores es registrado y se debe levantar una alerta independientemente de su estado de ejecución.

CÓMO AUDITARLO

CSC

- Verificar que se dispone de registros de auditoría que muestren cualquier cambio realizado en las imágenes de máquinas virtuales/contenedores.
- Asegurar que se registra a través del sistema de gestión de cambios todas las modificaciones en las imágenes.

CSP

- Identificar si el CSP dispone de portales que permitan la verificación de la integridad de las imágenes.
- Identificar los procesos de validación de la integridad de las imágenes y cómo se comunica esta información a los CSC.
- Revisar las cláusulas contractuales de seguridad al respecto.

RIESGO: Medidas de protección insuficientes a nivel de sistema.

DESCRIPCIÓN: Despliegue de sistemas con medidas de protección ineficaces, así como configuraciones inseguras que expongan la infraestructura a vulnerabilidades y ciberataques.

OBJETIVO DE CONTROL: Garantizar la correcta protección y bastionado de los sistemas dentro de la infraestructura en la nube, de forma que estén disponibles solamente los puertos, protocolos y servicios requeridos por negocio, y se apliquen otras medidas complementarias de seguridad como protección *antimalware*, cifrado, registro de *logs*, etc.

CÓMO AUDITARLO

CSC

- Revisar las guías de bastionado internas sobre las configuraciones de seguridad aplicadas a los sistemas operativos utilizados, incluyendo la lista de puertos, protocolos y servicios habilitados.
- Analizar las herramientas de seguridad integradas *(antimalware,* cifrado, registro de *logs,* etc.).

CSP

- Analizar la documentación que describa las guías de seguridad aplicadas, y su alineamiento con buenas prácticas y estándares (NIST o similar) correspondientes.
- Revisar las cláusulas contractuales de seguridad al respecto.

RIESGO: Control no adecuado de conectividades de los sistemas en la nube.

DESCRIPCIÓN: Falta de restricción de conexiones de tráfico externas e internas en los sistemas en la nube que puedan provocar accesos no autorizados, fuga de datos u otras amenazas de seguridad.

OBJETIVO DE CONTROL: Se dispone de una correcta restricción de conexiones entre los diferentes sistemas, instancias virtuales y entornos de red, pudiendo discernir entre confiables y no confiables, entrantes y salientes, internas y externas.

CÓMO AUDITARLO

CSC

- Revisar la políticas y procedimientos de configuración de red, incluyendo detalles sobre las listas de control de acceso (ACLs), reglas de firewall y segmentación de red.
- Analizar la documentación de la configuración de red actual, incluyendo ACLs, reglas de *firewall* y políticas de seguridad de red.
- Evidencias de los controles de red implementados y cómo estos complementan las configuraciones existentes.

CSP

- Documentación que describa las guías de seguridad aplicadas, y su alineamiento con buenas prácticas y estándares (NIST o similar) correspondientes.
- Revisar las cláusulas contractuales de seguridad al respecto.

RIESGO: Segmentación de red no adecuada en los entornos en la nube.

DESCRIPCIÓN: Falta de medidas de segmentación o aislamiento apropiadas en los diferentes entornos en la nube y sistemas *multi-tenant,* pudiendo llevar a la propagación de amenazas y afectar tanto al proveedor como a los diferentes clientes.

OBJETIVO DE CONTROL: Se dispone de una correcta segmentación de infraestructuras de red y sistemas *multi-tenant,* de forma que los entornos del proveedor y los clientes estén completamente aislados entre sí.

CÓMO AUDITARLO

CSC

- Verificar que se dispone de documentación de diseño y configuración que demuestre cómo se logra la segmentación de la red y el aislamiento de recursos.
- Solicitar evidencia de flujos de tráfico que aseguren la separación efectiva entre los entornos *multi-tenant* y el aislamiento de recursos.
- Solicitar evidencia de pruebas de penetración o evaluaciones de seguridad.

CSP

- Solicitar evidencia de pruebas de penetración o evaluaciones de seguridad que confirmen la efectividad de la segmentación y aislamiento.
- Revisar documentación técnica o guías de arquitectura que describan la segmentación de la red y el aislamiento de recursos para entornos *multi-tenant.*
- Revisar las cláusulas contractuales de seguridad al respecto.

RIESGO: Acceso de gestión con medidas de seguridad insuficientes.

DESCRIPCIÓN: Falta de medidas de seguridad adecuadas en el acceso de gestión hacia el hipervisor y consolas administrativas, de forma que pueda resultar en un acceso no autorizado al control de la infraestructura en la nube y sus sistemas y provocar la interrupción de operaciones y otros tipos de incidentes de seguridad.

OBJETIVO DE CONTROL: El acceso a todas las gestiones del hipervisor (o consolas administrativas de sistemas) está restringido al personal necesario, siguiendo el principio de mínimo privilegio, y protegido mediante controles técnicos como la autenticación multifactor (MFA), registros de auditoría, filtrado de direcciones IP, y comunicaciones seguras.

CÓMO AUDITARLO

CSC

- Revisar la documentación de las políticas de acceso que detallen los niveles de privilegio para el personal.
- Solicitar evidencia de la implementación de controles técnicos como MFA, filtrado de direcciones IP, y comunicaciones seguras.
- Listado de acceso a la gestión del hipervisor o a las consolas administrativas (origen, usuario, etc.).

CSP

- Verificar que se han realizado pruebas de penetración o evaluaciones de seguridad que confirmen la seguridad del acceso de gestión.
- Verificar que se dispone de documentación que describa cómo se protege el acceso a las consolas administrativas de la plataforma y cómo se monitoriza y audita este acceso.
- Revisar las cláusulas contractuales de seguridad al respecto.

RIESGO: Medidas de protección insuficientes a nivel de red.

DESCRIPCIÓN: Ausencia de medidas de seguridad adecuadas a nivel de red dentro de la infraestructura en la nube para proteger frente a ataques de red avanzados y disruptivos que puedan eludir medidas de seguridad más superficiales, comprometiendo la operación de la nube y sus servicios u otro tipo de incidentes de seguridad.

OBJETIVO DE CONTROL: Se dispone de mecanismos para la protección de la infraestructura de la red mediante el uso de medidas de defensa en profundidad *(Deep Packet Inspection,* Control de tráfico y *black-holing)* para la detección y respuesta a ataques en la red asociados con patrones de tráfico anómalos (ataques de suplantación de dirección MAC[20] y envenenamiento de ARP[21]) y/o ataques de denegación de servicio distribuidos (DDoS[22]).

20. Media Access Control.
21. Adress Resolution Protocol.
22. Distributed Denial of Service.

CÓMO AUDITARLO

CSC

- Verificar que se dispone de políticas y procedimientos de seguridad de red que incluyan medidas de defensa en profundidad *(Deep Packet Inspection,* control de tráfico y *black-holing).*
- Solicitar evidencia de herramientas y sistemas en uso para protección de DDoS.
- Solicitar y revisar los informes de incidentes o registros de auditoría que evidencien la detección y respuesta a ataques de red.

CSP

- Solicitar y revisar documentación descriptiva de las herramientas y técnicas de seguridad de red utilizadas para monitorizar y proteger la red.
- Revisar las cláusulas contractuales de seguridad al respecto.

7.4.5 RIESGOS EN EL REGISTRO Y MONITORIZACIÓN

RIESGO: Ausencia de tecnología necesaria para la gestión de *logs* y monitorización de eventos de seguridad de los entornos en la nube.

DESCRIPCIÓN: Medidas tecnológicas insuficientes para la recolección de *logs* o la monitorización y correlación apropiada de eventos de seguridad, en toda la infraestructura de red y sistemas dentro de la nube, pudiendo llevar a la incapacidad de detectar y responder a incidentes de seguridad.

OBJETIVO DE CONTROL: Garantizar la existencia de tecnologías de monitorización de seguridad necesarias para almacenar, analizar y correlacionar el mayor número de *logs* y eventos posibles de todos los segmentos de red y sistemas.

CÓMO AUDITARLO

CSC

- Verificar la existencia de un plan de monitorización para las plataformas en la nube, describiendo las áreas cubiertas, procedimientos implementados para la recolección y almacenamiento de *logs,* y las herramientas y técnicas específicas para la monitorización de eventos de seguridad, etc.

CSP

- Evidencias de la implementación de herramientas de monitorización de seguridad de red.
- Revisar las cláusulas contractuales de seguridad al respecto.

RIESGO: *Logs* insuficientes de los sistemas e infraestructura en la nube.

DESCRIPCIÓN: Generación incompleta de logs por parte de los sistemas de la nube, pudiendo llevar a la falta de visibilidad y trazabilidad de las acciones de seguridad críticas, y dificultando la detección temprana y la respuesta a incidentes de seguridad.

OBJETIVO DE CONTROL: Se recolectan todo tipo de eventos de seguridad (cambios de configuración, accesos sospechosos, borrado de *logs*, etc.) en todos los sistemas y puntos de la red, y a su vez estos son reenviados a un sistema centralizado.

CÓMO AUDITARLO

CSC

- Verificar las políticas y procedimientos en los que se definen los requerimientos de recolección de eventos en los distintos elementos tecnológicos.
- Verificar que se dispone de controles para monitorizar la correcta recolección de todos los eventos requeridos.
- Revisión de las herramientas de centralización de eventos de seguridad.

CSP

- Solicitar las políticas y procedimientos asociados a la recolección de eventos, y revisar en las herramientas utilizadas, la tipología de logs recolectados.
- Revisar las cláusulas contractuales de seguridad al respecto.

RIESGO: Falta de personal necesario para la monitorización de eventos de seguridad.

DESCRIPCIÓN: Ausencia de personal necesario para una monitorización de eventos de seguridad efectiva, provocando que actividades maliciosas o anómalas en la red pasen desapercibidas y sin respuesta debida.

OBJETIVO DE CONTROL: Se dispone de un equipo de monitorización de seguridad con la disponibilidad requerida para detectar comportamientos de red potencialmente sospechosos y/o anomalías en la red, así como roles y responsabilidades definidas que permita gestionar el proceso de alarmado para los diferentes eventos detectados, y se pueda comunicar con el equipo de respuesta ante incidentes si fuera necesario.

CÓMO AUDITARLO

CSC

- Revisar los procedimientos y políticas que demuestren la existencia de un equipo de monitorización de seguridad para las plataformas.
- Analizar los roles y responsabilidades definidos para la gestión de alarmas, matriz de escalado, criterio de severidad y la comunicación con el equipo de respuesta ante incidentes.

CSP

- Identificar la estructura organizativa, así como la definición de los roles para la monitorización de seguridad y la respuesta a eventos de seguridad.
- Revisar las cláusulas contractuales de seguridad al respecto.

RIESGO: Gestión inadecuada de los registros de seguridad.

DESCRIPCIÓN: Ausencia de medidas para asegurar la integridad y disponibilidad de los registros de seguridad, afectando así al cumplimiento legal, responsabilidad y rendición de cuentas, y la eficacia de las investigaciones forenses tras un incidente de seguridad.

OBJETIVO DE CONTROL: Se dispone de mecanismos de protección y criterios para la retención y la gestión del ciclo de vida de los registros de acuerdo con las obligaciones de cumplimiento legales y para respaldar las capacidades de investigación forense en caso de una violación de la seguridad.

CÓMO AUDITARLO

CSC

- Verificar las políticas y procedimientos para la protección y retención de registros de las plataformas, incluyendo el cumplimiento de las obligaciones legales.
- Revisar los procedimientos de acceso y autenticación de usuarios y evidencia de los mecanismos asociados para garantizar la protección de los registros y la cadena de custodia.

CSP

- Solicitar evidencia de los controles de acceso y autenticación de usuarios implementados.
- Revisar las cláusulas contractuales de seguridad al respecto.

RIESGO: Inexistencia de una fuente de tiempo única.

DESCRIPCIÓN: No disponer de una fuente temporal única, precisa y fiable provoca una falta de sincronización de eventos y *logs* de seguridad entre todos los sistemas de la nube, dificultando su correlación e investigación para reconstruir secuencias de incidentes.

OBJETIVO DE CONTROL: Se dispone de una fuente de tiempo externa fiable y mutuamente acordada para sincronizar los relojes del sistema de todos los sistemas, a fin de facilitar el seguimiento y la reconstitución de los plazos temporales.

CÓMO AUDITARLO

CSC

- Verificar que se dispone de documentación que demuestre la configuración de sincronización de tiempo en la infraestructura y cómo se mantiene la precisión del reloj del sistema.
- Revisar informes de trazas de la comunicación con la fuente de tiempo externa acordada.
- Solicitar evidencias de procedimientos de revisión y mantenimiento para asegurar la precisión continua del tiempo del sistema.

CSP

- Solicitar evidencias de la implementación de mecanismos de sincronización de tiempo y la precisión de los relojes del sistema.
- Revisar cláusulas contractuales de seguridad al respecto.

7.4.6 GESTIÓN DE INCIDENTES DE SEGURIDAD

RIESGO: Inadecuada gestión de los incidentes de seguridad.

DESCRIPCIÓN: No disponer de procesos adecuados para la gestión de incidentes de ciberseguridad, puede derivar en una respuesta tardía que puede hacer crecer de forma muy significativa su impacto operacional.

OBJETIVO DE CONTROL: Se dispone de procedimientos formalizados en los que se definen los controles necesarios para gestionar ciberincidentes. Estos contemplarían la detección, contención y su posterior análisis, así como si fueran necesarias acciones de comunicación a terceros debido a temas regulatorios.

CÓMO AUDITARLO

CSC

- Validar los procesos de monitorización y detección de incidentes de seguridad para asegurar que dichos procesos no se realizan de forma tardía o insuficiente en aquellos casos en los que el CSC mantiene la responsabilidad (sobre todo IaaS y parte de los servicios PaaS).
- Validar que los procesos de respuesta a ciberincidentes cubren todos los aspectos más relevantes, poniendo especial atención a una contención oportuna y efectiva.
- Asegurar que el CSC mantiene un registro completo de todos los incidentes producidos en los servicios cloud, y que estos son debidamente comunicados tanto internamente como externamente.

CSP

- Revisar los procedimientos de respuesta ante incidentes del CSP, analizando su completitud y adecuación a la tipología de servicios, así como asegurando la cobertura 24x7x365. A su vez, evidenciar los mecanismos de comunicación de los incidentes a los CSC.

RIESGO: Inadecuada gestión de los procesos de obtención de evidencias asociadas a un incidente.

DESCRIPCIÓN: No disponer de procesos adecuados para la gestión del descubrimiento y obtención de evidencias electrónicas *(E-Discovery)* puede derivar en que durante el proceso de *E-Discovery* en la nube, terceros no autorizados accedan a datos sensibles o confidenciales, lo que podría generar riesgos legales y reputacionales a la Organización..

OBJETIVO DE CONTROL: Se dispone de procedimientos formalizados en los que se definan los controles necesarios para los procesos de *E-Discovery* en la nube, que aseguren la privacidad de datos sensibles y el cumplimiento con los requisitos legales y regulatorios ante procesos de *E-Discovery.*

CÓMO AUDITARLO

CSC - CSP

- Identificar que los procesos de gestión de *E-Discovery* minimizan los riesgos de accesos a datos sensibles o confidenciales por parte de terceros no autorizados en todos aquellos servicios desplegados en formato IaaS, PaaS y SaaS.
- Dicho control debe revisarse tanto en el CSC como en el CSP si ambos realizan proceso de *E-discovery,* o únicamente en el CSP si dicho control es efectuado únicamente por el proveedor.

RIESGO: Inadecuada preservación de la información obtenida durante el análisis de incidentes.

DESCRIPCIÓN: La informática forense en la nube presenta desafíos únicos en términos de preservación y recuperación de la evidencia digital, lo que puede afectar la integridad de la investigación y el análisis forense. Durante las investigaciones forenses en la nube, existe el riesgo de que los datos forenses sean comprometidos o accedidos por terceros no autorizados, lo que podría comprometer la validez de la investigación y la confidencialidad de la información.

OBJETIVO DE CONTROL: Se dispone de procedimientos formalizados en los que se definan los controles necesarios para asegurar la preservación, recuperación e integridad de la evidencia digital para la realización de análisis forenses. Además, estos controles deben de asegurar la validez de las evidencias digitales en caso de ser requeridas en procesos legales.

CÓMO AUDITARLO

CSC - CSP

- Identificar que los procesos de gestión para la preservación, recuperación e integridad de las evidencias digitales para la realización de análisis forenses son adecuados y operan de forma eficaz en los sistemas que soportan los servicios tipo IaaS, PaaS y SaaS. Además, estos controles deben asegurar la validez de las evidencias digitales en caso de ser requeridas en procesos legales.
- Dicho control debe revisarse tanto en el CSC como en el CSP si ambos conservan las evidencias, o únicamente en uno de ellos, si las evidencias solamente han sido conservadas por una de las partes.

7.4.7 GESTIÓN DE VULNERABILIDADES

RIESGO: Inadecuada evaluación y gestión de vulnerabilidades en los sistemas del CSP o del CSC.

DESCRIPCIÓN: No disponer de procesos adecuados para la detección y respuesta a vulnerabilidades, puede exponer a la organización a ataques que puedan comprometer los sistemas y la información.

OBJETIVO DE CONTROL: Se dispone de procedimientos formalizados en los que se definan las tipologías de revisiones para identificar y categorizar vulnerabilidades, así como el proceso de gestión de los resultados, considerando la priorización de las vulnerabilidades, en base a su criticidad; el tiempo de resolución (calendario); los procesos de excepción; así como la definición de métricas, monitorización y reporte asociado, incluida la utilización de bibliotecas externas de vulnerabilidades.

CÓMO AUDITARLO

CSC

- **En los servicios IaaS y PaaS:** Verificar que los procedimientos y procesos de gestión de vulnerabilidades internos consideran el escaneo de los componentes gestionados por el CSP, así como una priorización de actualización en función de la criticidad de las vulnerabilidades, y que se monitoriza tanto el cumplimiento de los tiempos de resolución, como las posibles excepciones. Es necesario asegurar que los tiempos de resolución dictaminados en función de la criticidad, no distinguen si la vulnerabilidad es de un activo cloud u *on-premise.*
- **En los servicios SaaS:** Los clientes pueden afrontar dificultades para monitorear y gestionar adecuadamente las amenazas y vulnerabilidades en los servicios en la nube, debido a la falta de visibilidad y control sobre la infraestructura subyacente. Se deben exigir estos procedimientos y auditorías técnicas previamente a la formalización de contratos con proveedores de servicios en la nube.

CSP

- Evaluar los procesos de gestión de vulnerabilidades de los CSP, analizando la tipología de revisiones, la periodicidad de estas, así como la gestión de las vulnerabilidades identificadas en base a su criticidad y evaluar el cumplimiento de los procesos establecidos para una muestra de activos y vulnerabilidades.
- Identificar los procesos de excepción y evaluar su cumplimiento para una muestra de vulnerabilidades.
- Evaluar los mecanismos de monitorización y *reporting* de las vulnerabilidades identificadas.

RIESGO: Inadecuada gestión de parches y actualizaciones en los sistemas del CSP o del CSC.

DESCRIPCIÓN: No disponer de procesos adecuados para la detección y respuesta a vulnerabilidades, puede exponer a la organización a ataques que puedan comprometer los sistemas y la información..

OBJETIVO DE CONTROL: Se dispone de políticas y procedimientos formalizados de los procesos continuos de parcheado, configuraciones de seguridad, actualizaciones, así como de una correcta monitorización de los entornos y su posterior *reporting*.

CÓMO AUDITARLO

CSC

- **En los servicios IaaS y PaaS:** Analizar que existen procedimientos y procesos de actualización y parcheado continuo por parte del CSC, y éstos se mantienen al día según los diferentes proveedores externos de software. A su vez, verificar que los ciclos asociados a dichos procesos están alineados con los vinculados a los activos internos de la organización.

CSP

- En cualquier modalidad de servicio, analizar que existen procedimientos y procesos de actualización y parcheado continuo por parte del CSP, y que éstos se mantienen al día según los diferentes proveedores externos de *software*.

RIESGO: Inadecuada configuración de seguridad.

DESCRIPCIÓN: No disponer de unas líneas base de configuración de seguridad para los distintos elementos tecnológicos, puede exponer a la organización a ataques que puedan comprometer los sistemas y la información.

OBJETIVO DE CONTROL: Se dispone de procedimientos y procesos para la maquetación y preparación de configuraciones de seguridad en los sistemas involucrados, así como la eliminación de cuentas de acceso locales y otros servicios no utilizados.

CÓMO AUDITARLO

CSC

- **En los servicios IaaS y PaaS:** Asegurar que existen procedimientos y procesos establecidos con la definición y revisión de configuraciones base de seguridad y que éstas siguen las mejores prácticas de las guías de configuración segura existentes y la utilización de plantillas. Verificar que los ciclos asociados a dichos procesos están alineados con los vinculados a los activos internos de la organización.

CSP

- En cualquier modalidad de servicio, es necesario asegurar que existen procedimientos y procesos establecidos con la definición y revisión de configuraciones base de seguridad y que éstas siguen las mejores prácticas de las guías de configuración segura existentes y la utilización de plantillas.

7.4.8 CONTROL DE ACCESO

RIESGO: Políticas y procedimientos de control de acceso incompletos.

DESCRIPCIÓN: Si las políticas y procedimientos de acceso no son lo suficientemente estrictos en términos de seguridad, o no se aplican de forma rigurosa, puede dar lugar a flujos de autenticación inconsistentes, credenciales débiles, insuficiente monitorización de las cuentas, etc., lo que puede terminar en un acceso no autorizado con sabotaje, filtración de datos y otros actos maliciosos.

OBJETIVO DE CONTROL: Se dispone de políticas y procedimientos que garantizan un control de acceso seguro, incluyendo aspectos como, el ciclo de vida de cuentas de usuario, gestión segura de las contraseñas, métodos de autenticación robustos, segregación de funciones, principio de mínimo privilegio, etc.

CÓMO AUDITARLO

CSC

- Evaluar las políticas y procedimientos que describan las medidas relativas al control de acceso, gestión de contraseñas, ciclo de vida de cuentas de usuario, sistemas de autenticación reforzada, matriz RACI, etc, propios de la organización.
- Dichas políticas deben considerar las particularidades de las distintas modalidades de servicios en la nube.

CSP

- Evaluar los procedimientos propios del CSP, y asegurar que los requerimientos definidos en el mismo tienen como mínimo el mismo nivel de control que el requerido en los procedimientos internos del CSC.

RIESGO: Control inadecuado de las cuentas privilegiadas.

DESCRIPCIÓN: No controlar adecuadamente las cuentas de usuario con privilegios elevados puede derivarse en accesos no autorizados al entorno de administración de los sistemas en la nube, así como a información sensible que estos puedan almacenar, tratar o transmitir.

OBJETIVO DE CONTROL: Se gestiona el acceso de cuentas privilegiadas mediante una herramienta centralizada integrada con los sistemas del entorno de la nube, que permita un acceso de administración homogéneo, gestión segura de las credenciales de estas cuentas, así como registros de actividad.

CÓMO AUDITARLO

CSC	CSP
- Evaluar las políticas y procedimientos referentes a cómo se gestionan las cuentas privilegiadas en el CSC.	- Evaluar las políticas y procedimientos referentes a como se gestionan las cuentas privilegiadas en el CSP.
- Revisar el flujo de autorización de usuarios a solicitar cuentas privilegiadas, así como el proceso de solicitud y revocación.	- Revisar el flujo de autorización de usuarios a solicitar cuentas privilegiadas, así como el proceso de solicitud y revocación.
- Revisar que los usuarios integrados en las herramientas de gestión se corresponden con los de los sistemas, y que no hay usuarios fuera de las mismas.	- Revisar que los usuarios integrados en las herramientas de gestión se corresponden con los de los sistemas, y que no hay usuarios fuera de las mismas.
- Revisar el proceso de rotado de las contraseñas y/o de desvinculación de usuarios.	- Revisar el proceso de rotado de las contraseñas y/o de desvinculación de usuarios.

RIESGO: Control inadecuado de las identidades de usuario.

DESCRIPCIÓN: No controlar adecuadamente las identidades de usuario puede resultar en la asignación de roles equivocados, la herencia de roles errónea tras un cambio de funciones, o la no eliminación de cuentas de usuarios que han abandonado la organización, pudiendo terminar en una exposición excesiva y no deseada de los diferentes recursos e información de la infraestructura en la nube.

OBJETIVO DE CONTROL: Gestionar las identidades de usuario mediante el uso de una herramienta centralizada que se integre con el resto de los sistemas de las unidades de negocio, permitiendo una automatización de la provisión, actualización y eliminación (deprovisión) de las identidades y sus roles.

CÓMO AUDITARLO

CSC	CSP
- Evaluar las políticas y procedimientos referentes al ciclo de vida de identidades de usuario en el CSC.	- Evaluar las políticas y procedimientos referentes al ciclo de vida de identidades de usuario en el CSP.
- Evidenciar el flujo de provisión (y deprovisión) de identidades, diagramas de la arquitectura, listado de entidades creados en la herramienta IAM, etc. en el CSC.	- Evidenciar el flujo de provisión (y deprovisión) de identidades, diagramas de la arquitectura, listado de entidades creados en la herramienta IAM, etc. en el CSP.

Consideraciones finales

Las organizaciones, en su estrategia de transformación digital y de búsqueda de mejoras en la eficiencia en los procesos tecnológicos, están incorporando de forma significativa la adopción de tecnologías y servicios en la nube. El principal objetivo de este proceso es el ahorro de costes, pero a la vez se busca que dicha transformación conlleve mejoras en las medidas de seguridad, en los niveles de disponibilidad, así como una mayor capacidad para afrontar las exigencias tecnológicas del mercado. En consecuencia, los riesgos derivados de la externalización de Tecnologías de la Información) hacia proveedores de servicios en la nube (CSP), están creciendo a la vez que aumentan las exigencias legislativas y de regulaciones sectoriales.

En este contexto, Auditoría Interna tiene un rol relevante, no solamente en su función de aseguramiento, si no en la búsqueda de un asesoramiento y acompañamiento continuo, tanto en las fases iniciales de la transformación, como en fases posteriores.

En su rol de aseguramiento, en organizaciones con un alto grado de adopción de tecnologías en la nube, se debe disponer de revisiones específicas, tanto del propio modelo de gobierno de la nube que dispone la organización, como de los servicios más relevantes que hayan sido externalizados parcial o totalmente a algún CSP. Para ello, es de vital importancia definir una estrategia de revisión adecuada e incluir en la planificación anual revisiones que permitan cubrir los riesgos más relevantes.

En el rol de asesoramiento, sobre todo en organizaciones en proceso de transición a la nube, Auditoría Interna debe apoyar en la identificación de los principales riesgos, tanto de los proyectos de migración, como de las primeras fases de la operación en el nuevo contexto.

En definitiva, Auditoría Interna debe formar parte tanto del proceso de transición a la nube, como de la monitorización continua posterior.

Glosario de términos

Los principales elementos tecnológicos que componen los diferentes servicios en la nube son:

- **Virtualización**
  Creación de máquinas virtuales (VM) y recursos informáticos virtualizados, como redes y almacenamiento.
- **Redes y comunicaciones**
  La infraestructura de red en la nube incluye switches, routers, balanceadores de carga y otros dispositivos para enrutar el tráfico de manera eficiente.
- **Centro de datos**
  Múltiples centros de datos distribuidos en diferentes zonas geográficas, incluyendo diferentes países.
- **Almacenamiento**
  Sistemas de almacenamiento distribuido.
- **Procesamiento en la nube**
  La computación en la nube incluye capacidades de procesamiento, memoria y potencia de cálculo proporcionadas bajo demanda.
- **Orquestación y gestión de recursos**
  Esencial para administrar y coordinar la implementación, escalado y mantenimiento de aplicaciones y servicios.
- **Seguridad**
  Abarca la protección de datos, la gestión de identidades y accesos, el cifrado, la detección de amenazas, entre otros aspectos de la seguridad de la información.
- **Monitorización y análisis**
  Capacidades de monitorización y análisis para supervisar el rendimiento, la disponibilidad y la seguridad de los servicios.

Bibliografía

- MONOGRAFÍAS
  - **PÉREZ Roger, DE PALMA Javier.** *Auditoría Interna de los Servicios en la Nube. Normas, metodologías y marcos de referencia.* Jornadas de Auditoría Interna del IAI de España, 2023.

- INFORMES Y ESTUDIOS
  - **European Union Agency for Cybersecurity.** *Cloud Service - Scheme.* 2020.
  - **SALAZAR, Diana.** *Cloud Security Framework Audit Methods,* 25th April 2016.
  - **Committee of Sponsoring Organizations of the Treadway Commission (COSO),** *Enterprise Risk Management for Cloud Computing,* July 2021.
  - **Certificate in Cloud Auditing Knowledge (CCAK).**

- NORMAS
  - **Parlamento Europeo.** *Directive on measures for a high common level of cybersecurity across the Union (NIS2).* 2022/2555, 2022.
  - **Parlamento Europeo.** *Reglamento sobre la resiliencia operativa digital del sector financiero (DORA).* 2022/2554, 2022.
  - **Parlamento Europeo.** *Reglamento relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD).* 2016/679, 2016.
  - **Ministerio de Asuntos Económicos y Transformación Digital.** *Real Decreto por el que se regula el Esquema Nacional de Seguridad. (ENS).* 311/2022, 2022.
  - **International Organization for Standardization (ISO).** *Information Security, cybersecurity and privacy protection - Information security Management systems - Requirements.* ISO/IEC 27001:2022, 2022.
  - **International Organization for Standardization (ISO).** *Information technology - security techniques - Code of practice for information security controls base don ISO/IEC 27002 for cloud services.* ISO/IEC 27017:2015, 2015.
  - **Cloud Security Alliance (CSA).** *Cloud Control Matrix v4.0,* 2021.
  - **National Institute of Standards and Technology (NIST).** *The NIST Cybersecurity Framework (CSF) 2.0,* 2024.
  - **National Institute of Standards and Technology (NIST).** *Guidelines on Security and Privacy in Public Cloud Computing. NIST SP 800-144,* 2011.
  - **National Institute of Standards and Technology (NIST).** *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. NIST SP 800-37 Rev.2,* 2018.
  - **Committee of Sponsoring Organizations of the Treadway Commission (COSO).** *Enterprise Risk Management for Cloud Computing.*

- ARTÍCULOS DE REVISTA
  - **SHIRLEY M. Radack.** "Cloud Computing: A Review of Features, Benefits, and Risks, and Recommendations for Secure, Efficient Implementations". *ITL Bulletin.* June 27, 2012.

Instituto de Auditores Internos de España

Santa Cruz de Marcenado, 33 · 28015 Madrid · Tel.: 91 593 23 45 · Fax: 91 593 29 32 · www.auditoresinternos.es

ISBN: 978-84-129298-2-9

Maquetación: desdecero, estudio gráfico

OTRAS PRODUCCIONES DE LA FÁBRICA DE PENSAMIENTO

AUDITORÍA INTERNA DE LA INTELIGENCIA ARTIFICIAL APLICADA A PROCESOS DE NEGOCIO

Aborda los casos de uso más comunes de la Inteligencia Artificial (IA) en procesos empresariales y la regulación aplicable promovida por los legisladores. Además, describe los principales modelos y tipologías de IA, incluyendo la nueva perspectiva de la Inteligencia Artificial generativa, que la industria está desarrollando.

AUDITORÍA INTERNA DE PROCESOS ROBOTIZADOS DE NEGOCIO

Se presentan los diferentes tipos de robotización de procesos del negocio y los distintos roles que puede asumir Auditoría Interna (aseguramiento y asesoramiento) frente a una tecnología que está cada vez más presente en la operativa de las empresas y que presenta oportunidades, pero también riesgos que hay que gestionar y minimizar.

AUDITORÍA INTERNA DEL PROCESO DE INVERSIÓN EN TECNOLOGÍAS EMERGENTES

Este documento incluye información para comprender mejor qué son y cómo evolucionan las tecnologías emergentes, el posicionamiento de Auditoría Interna frente a esas nuevas tecnologías, y un análisis de riesgos en una auditoría interna de inversiones en tecnologías emergentes.

LA FÁBRICA DE PENSAMIENTO
INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA

Los servicios en la nube ofrecen numerosas ventajas a las organizaciones, pero también implican la necesaria evaluación y mitigación de los riesgos asociados a esta tecnología, sobre los que Auditoría Interna debe asegurar que las organizaciones cuentan con los mecanismos necesarios para la gestión de estos riesgos a través de la realización de revisiones sobre estos entornos. De esta forma, el documento se configura como una guía útil y práctica para los auditores internos, que les ayude a afrontar con éxito los retos que plantea esta parte del proceso de transformación digital de las organizaciones.

Instituto de Auditores Internos de España
The Institute of Internal Auditors