

SIEMPRE CIBERSEGURO, NUNCA CIBER-INSEGURO: AUDITANDO LA TORMENTA DE LA NUBE

FERNEY ALVARADO
VICEPRESIDENTE ISACA MEDELLÍN

VII

**Encuentro
Latinoamericano
de Auditoría**

Conocimiento y aplicación en la era digital



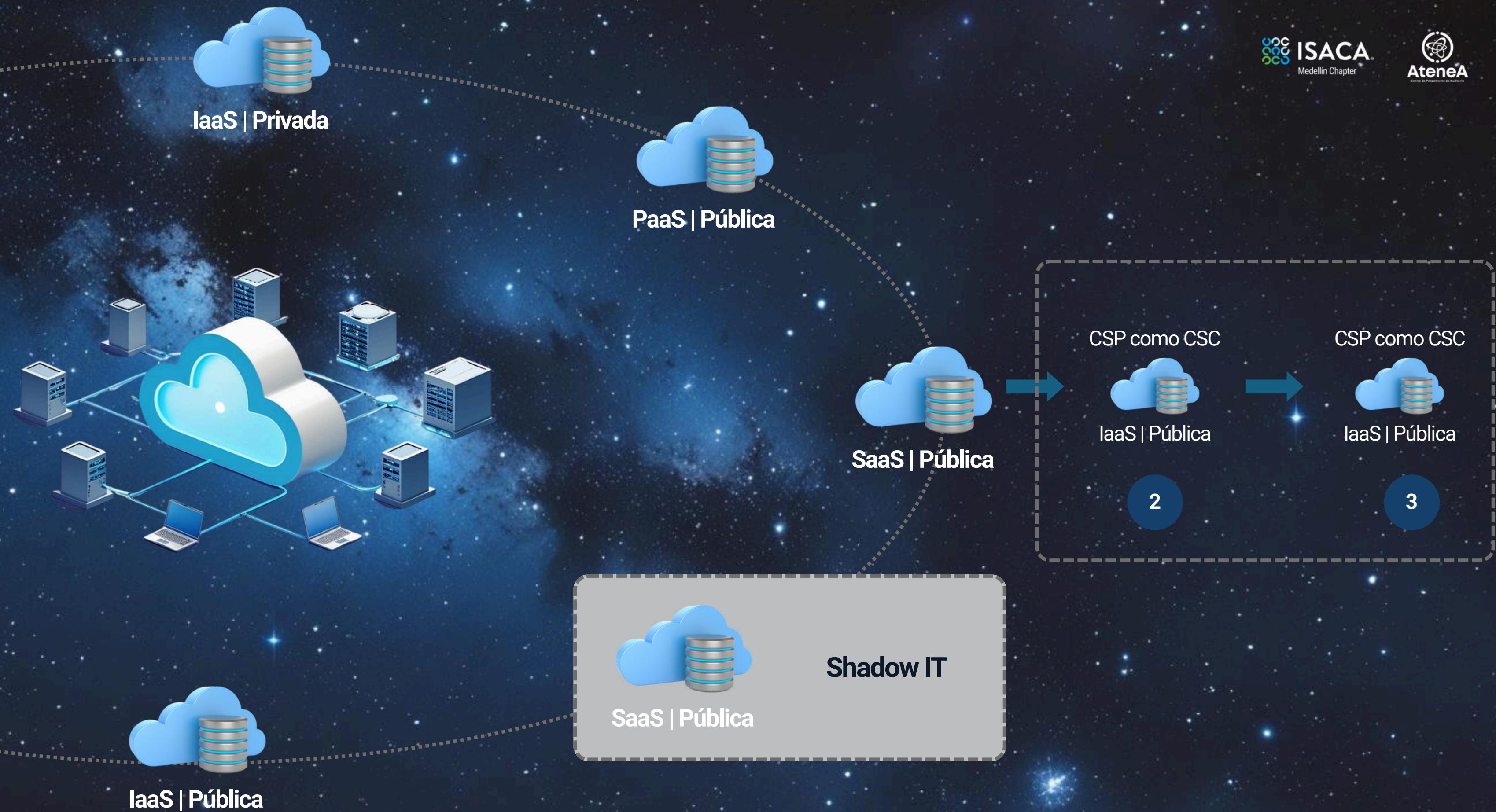


**ANTES DE INICIAR UN PROYECTO
(O CONFERENCIA)...**

**COMPRUEBA SI DISPONES DE
RECURSOS**



Tecnología que permite prestar una serie de servicios a través de una red, en la mayoría de los casos, a través de Internet.



Modelo de Servicio
IaaS, PaaS y SaaS

Modelo de Implementación:
Privada, pública, comunitaria e híbrida

CSC:
Cloud Service Customer

CSP:
Cloud Service Provider

MODELO DE RESPONSABILIDAD COMPARTIDA

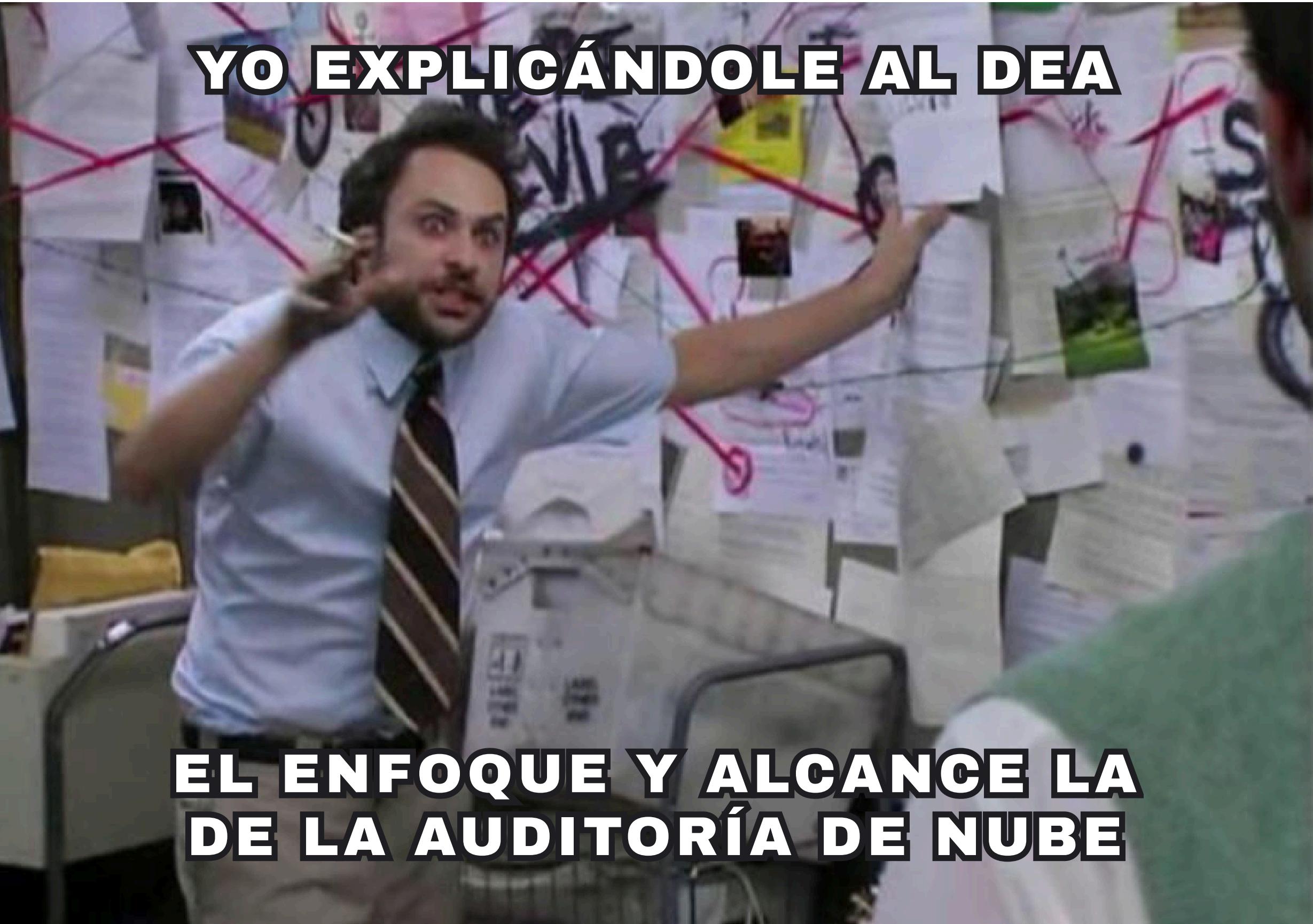


CSP
Cloud Service Provider



CSC
Cloud Service Customer

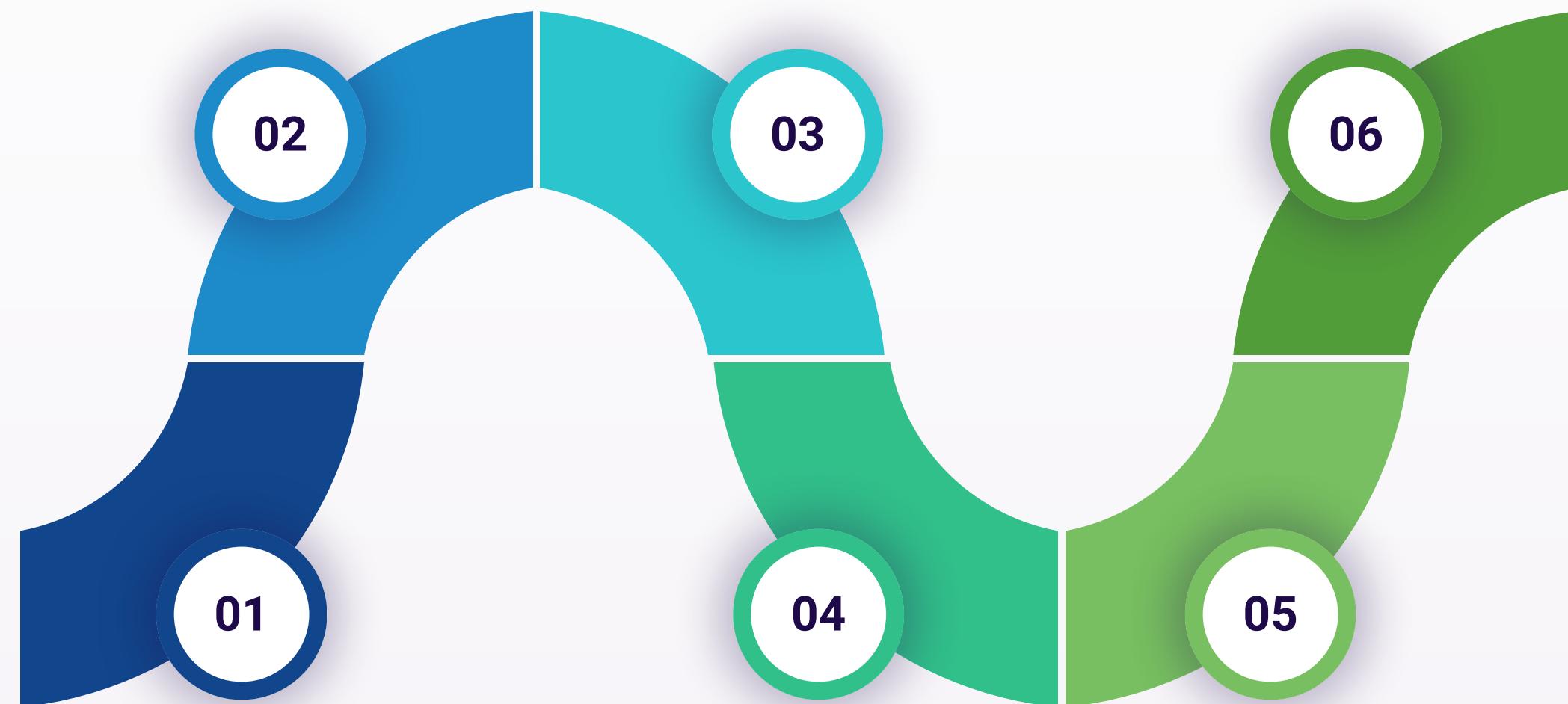
Y ENTONCES...
¿QUÉ AUDITAMOS?



Riesgos

Enfoque y alcance

Resultados e informe

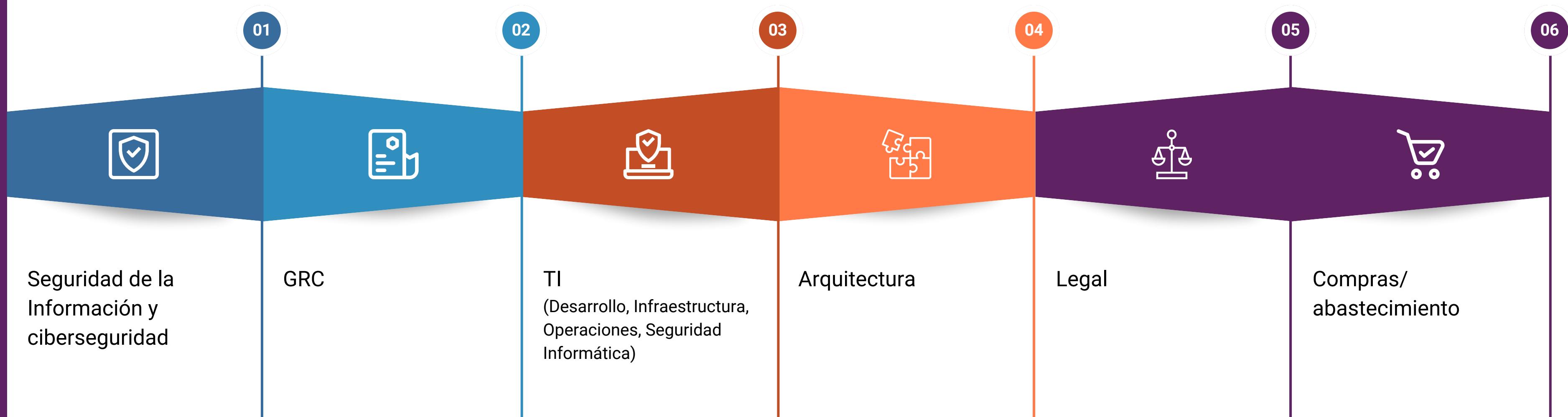
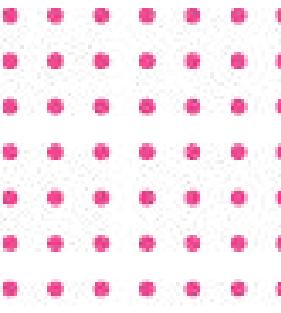


**Inventario de
servicios de nube**

**Programa de trabajo
(guías)**

Ejecución

ACTORES MÁS RELEVANTES



Regulación: LEPDP - C.E 005 de 2019 SFC - C.E 007 de 2018 SFC - PCI - RGPD



¿CÓMO OBTENEMOS UN INVENTARIO ACTUALIZADO Y COMPLETO?

- Solicitar inventarios de nube a: Seguridad de la Información, Arquitectura, TI, Compras, Legal y cumplimiento.
- Conocimiento de los procesos de negocio y las herramientas que utilizan para su funcionamiento.
- CASB, CMDB, Consolas de facturación.
- Generar reporte auxiliar de la cuenta contable donde se registran los pagos de licenciamiento/herramientas tecnológicas.

INVENTARIO DE SERVICIOS DE NUBE

Nombre del Servicio	Modelo de Servicio (IaaS/PaaS/SaaS)	Proceso del negocio	Propietario Interno	Proveedor	Modelo de Implementación	Fecha de Vencimiento Contrato	SLA Disponibilidad
Amazon S3	IaaS	TI	Jefe Infraestructura	AWS	Pública	2026-12-31	SLA 99.9%
Azure SQL	PaaS	Finanzas	Gerente de Finanzas	Microsoft Azure	Híbrida	2025-11-30	SLA 99.95%
Google Workspace	SaaS	Toda la empresa	CIO	Google	Pública	2027-06-15	SLA 99.9%
Salesforce CRM	SaaS	Comercial	Gerente Comercial	Salesforce	Pública	2026-08-01	SLA 99.9%
SAP S/4HANA Cloud	SaaS	Finanzas	CFO	SAP	Privada	2028-01-01	SLA 99.99%
Office 365	SaaS	Toda la empresa	CIO	Microsoft	Pública	2027-04-01	SLA 99.9%
Dropbox Business	SaaS	Marketing	CMO	Dropbox	Pública	2025-07-20	SLA 99.9%
AWS EC2	IaaS	TI	Infra Manager	AWS	Pública	2026-09-15	SLA 99.99%
Oracle Cloud ERP	SaaS	Finanzas	CFO	Oracle	Híbrida	2028-12-31	SLA 99.95%
GitHub Enterprise	SaaS	TI	Líder DevOps	GitHub/Microsoft	Pública	2027-03-10	SLA 99.9%

Nombre del Servicio	Clasificación de la Información	Ubicación de Datos	Certificaciones Cumplidas	Reportes de Auditoría Disponibles	Integraciones Clave	Costo Mensual (USD)
Amazon S3	Confidencial	EE.UU.	ISO 27001, SOC 2	SOC 2	ERP, DataLake	\$ 1.200,00
Azure SQL	Crítica	Brasil	ISO 27018	SOC 1, SOC 2	ERP Financiero	\$ 2.500,00
Google Workspace	Sensible	EE.UU.	ISO 27017	SOC 3	Integrado con CRM	\$ 5.000,00
Salesforce CRM	Confidencial	EE.UU.	SOC 2, GDPR	SOC 2	ERP, BI	\$ 7.000,00
SAP S/4HANA Cloud	Crítica	Alemania	ISO 27001, SOC 1	ISAE 3402	ERP Core	\$ 15.000,00
Office 365	Sensible	EE.UU./Brasil	ISO 27017	SOC 2	Teams, SharePoint	\$ 6.000,00
Dropbox Business	Confidencial	EE.UU.	ISO 27001	SOC 2	Integración Google Workspace	\$ 1.000,00
AWS EC2	Sensible	EE.UU.	ISO 27001	SOC 2	ERP, DataLake	\$ 10.000,00
Oracle Cloud ERP	Crítica	EE.UU./Canadá	SOC 1, SOC 2	SOC 2	ERP	\$ 12.000,00
GitHub Enterprise	Sensible	EE.UU.	ISO 27001	SOC 2	CI/CD	\$ 2.000,00

RIESGOS DE LAS NUBES



1



GOBIERNO DE
NUBE

2



SELECCIÓN Y
CONTRATACIÓN
DE LA NUBE

3



CONTROLES
EN EL CSP

4



CONTROLES
EN EL CSC

5



CUMPLIMIENTO
LEGAL Y REGULATORIO

6

ESQUEMA COMBINADO

POSIBLES ENFOQUES DE AUDITORÍA

Cloud Controls Matrix (CCM)

Version 4 of the CCM and CAIQ
are now combined!

[Download CCM and CAIQ](#)



17 DOMINIOS

A&A	Audit & Assurance	IAM	Identity & Access Management
AIS	Application & Interface Security	IPY	Interoperability & Portability
BCR	Business Continuity Mgmt & Op Resilience	IVS	Infrastructure & Virtualization Security
CCC	Change Control & Configuration Management	LOG	Logging & Monitoring
CEK	Cryptography, Encryption, & Key Management	SEF	Sec. Incident Mgmt, E-Disc & Cloud Forensics
DCS	Datacenter Security	STA	Supply Chain Mgmt, Transparency, & Accountability
DSP	Data Security & Privacy	TVM	Threat & Vulnerability Management
GRC	Governance, Risk Management, & Compliance	UEM	Universal Endpoint Management
HRS	Human Resources Security		

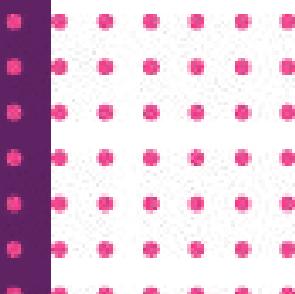
CCM CONTROLS

Cloud Controls Matrix v4.0.13							
						Typical Control Applicability and Ownership	
Control Domain	Control Title	Control ID	Control Specification	CCM Lite	IaaS	PaaS	SaaS
Infrastructure & Virtualization Security - IVS							
Infrastructure & Virtualization Security	Infrastructure and Virtualization Security Policy and Procedures	IVS-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for infrastructure and virtualization security. Review and update the policies and procedures at least annually.	No	Shared	CSP-Owned	CSP-Owned
Infrastructure & Virtualization Security	Capacity and Resource Planning	IVS-02	Plan and monitor the availability, quality, and adequate capacity of resources in order to deliver the required system performance as determined by the business.	No	CSP-Owned	CSP-Owned	CSP-Owned
Infrastructure & Virtualization Security	Network Security	IVS-03	Monitor, encrypt and restrict communications between environments to only authenticated and authorized connections, as justified by the business. Review these configurations at least annually, and support them by a documented justification of all allowed services, protocols, ports, and compensating controls.	Yes	Shared	Shared	CSP-Owned
Infrastructure & Virtualization Security	OS Hardening and Base Controls	IVS-04	Harden host and guest OS, hypervisor or infrastructure control plane according to their respective best practices, and supported by technical controls, as part of a security baseline.	Yes	Shared	CSP-Owned	CSP-Owned
Infrastructure & Virtualization Security	Production and Non-Production Environments	IVS-05	Separate production and non-production environments.	No	Shared	Shared	Shared
Infrastructure & Virtualization Security	Segmentation and Segregation	IVS-06	Design, develop, deploy and configure applications and infrastructures such that CSP and CSC (tenant) user access and intra-tenant access is appropriately segmented and segregated, monitored and restricted from other tenants.	Yes	Shared	Shared	CSP-Owned

CCM IMPLEMENTATION GUIDELINES

CCM™ CLOUD CONTROLS MATRIX v4.0.13

Control Domain	Control Title	Control ID	Control Specification	Control Ownership by Service Delivery Model			CCM Implementation Guidelines v2.0	
				IaaS	PaaS	SaaS	CSP	CSC
Human Resources	Personnel Roles and Responsibilities	HRS-09	Document and communicate roles and responsibilities of employees, as they relate to information assets and security.	Shared (Independent)	Shared (Independent)	Shared (Independent)	<p>Control Ownership Rationale. The determination for this control objective remains the same regardless of the cloud architecture adoption; fundamentally this control is shared between both the CSC and the CSP. The controls however are independent from one another. Both entities should document and communicate the roles and responsibilities of employees, as they relate to information assets, privacy, and security.</p> <p>Implementation Guidelines. Applicable to all service models: The CSP should identify, define, document, and communicate information-asset protection guidance and responsibilities. These should be reviewed and updated annually.</p> <p>All employees, contractors, and contingent staff should receive role-based security training commensurate with their access, duties, and responsibilities at the start of their service agreement before granting them access to corporate facilities, resources, and assets and annually thereafter. Changes to relevant policies should be communicated to employees, contractors, and contingent staff.</p>	<p>Control Ownership Rationale. The control ownership rationale provided for the CSP applies.</p> <p>Implementation Guidelines. Applicable to all service models: The CSC should identify, define, document, and communicate information asset protection guidance and responsibilities. These should be reviewed and updated annually.</p> <p>All employees, contractors, and contingent staff should receive role-based security training commensurate with their access, duties, and responsibilities at the start of their service agreement before granting them access to corporate facilities, resources, and assets and annually thereafter. Changes to relevant policies should be communicated to employees, contractors, and contingent staff.</p>



CCM AUDITING GUIDELINES



Control Domain	Control Title	Control ID	Control Specification	Auditing Guidelines
Application & Interface Security - AIS				
Application & Interface Security	Application and Interface Security Policy and Procedures	AIS-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for application security to provide guidance to the appropriate planning, delivery and support of the organization's application security capabilities. Review and update the policies and procedures at least annually.	<ol style="list-style-type: none"> 1. Examine policy and procedures for adequacy, approval, communication, and effectiveness as applicable to planning, delivery, and support of the organization's application security capabilities. 2. Examine policy and procedures for evidence of review at least annually.
Application & Interface Security	Application Security Baseline Requirements	AIS-02	Establish, document and maintain baseline requirements for securing different applications.	<ol style="list-style-type: none"> 1. Examine policy and procedures for adequacy and effectiveness. 2. Determine if security baseline requirements of respective applications are clearly defined. 3. Examine the process to determine the baseline for an application.
Application & Interface Security	Application Security Metrics	AIS-03	Define and implement technical and operational metrics in alignment with business objectives, security requirements, and compliance obligations.	<ol style="list-style-type: none"> 1. Examine policy and procedures for definition of operational metrics, security, and compliance requirements.
Application & Interface Security	Secure Application Design and Development	AIS-04	Define and implement a SDLC process for application design, development, deployment, and operation in accordance with security requirements defined by the organization.	<ol style="list-style-type: none"> 1. Examine policy and procedures for definition of SDLC (Software Development Lifecycle), security, and compliance requirements. 2. Examine the state of implementation of the SDLC process. 3. Verify that the SDLC implementation is in accordance with requirements.
Application & Interface Security	Automated Application Security Testing	AIS-05	Implement a testing strategy, including criteria for acceptance of new information systems, upgrades and new versions, which provides application security assurance and maintains compliance while enabling organizational speed of delivery goals. Automate when applicable and possible.	<ol style="list-style-type: none"> 1. Examine policy and procedures for definition of testing strategies, automation of security testing, and change management. 2. Determine security assurance and acceptance criteria for the new information system(s). 3. Determine if the software release process is automated where applicable.

MARCOS, GUÍAS, PROGRAMAS...



Auditoría Interna
de la gestión
operativa
del Cloud



¡Hola GPT!

Como contexto, se está realizando una auditoría de nube a una compañía Colombiana, del sector financiero, vigilada por la Superintendencia Financiera de Colombia y que tiene operaciones en otros países de Suramérica como Brasil y Panamá.

Por favor:

1. Toma el inventario de servicios de nube y filtra aquellos servicios que en la columna "Clasificación de la Información" tengan información "Sensible".
2. Para cada servicio seleccionado en el filtro del punto 1, determina:
 - a. Los principales 3 riesgos, teniendo en cuenta el modelo de servicio, modelo de implementación, ubicación de los datos y demás.
 - b. De acuerdo con el modelo de servicio de los servicios de nube filtrados, toma del archivo CCM, de la hoja llamada "CCM", los principales controles, así:
 - Si es IaaS, filtra la columna 6 donde el control sea compartido (shared) y a cargo del proveedor (CSP-Owned).
 - Si es SaaS, filtra la columna 8 donde el control sea compartido (shared) y a cargo del proveedor (CSP-Owned).
 - c. A partir de los controles seleccionados en el numeral B, toma de la hoja "Auditing Guidelines" la prueba que se debe realizar (columna 5), indicando el paso a paso de la prueba con la traducción al español, comparando el ID de control tomado de la hoja "CCM" (columna 3) y el ID de control de la hoja "Auditing Guidelines" (columna 3).
 - d. Y en la hoja "Scope Applicability (Mappings)" trae el mapeo del control seleccionado en la CCM con CIS v8.0 y del archivo CIS_Controls_v8_Spanish trae un resumen del control.



Pensó durante 12s

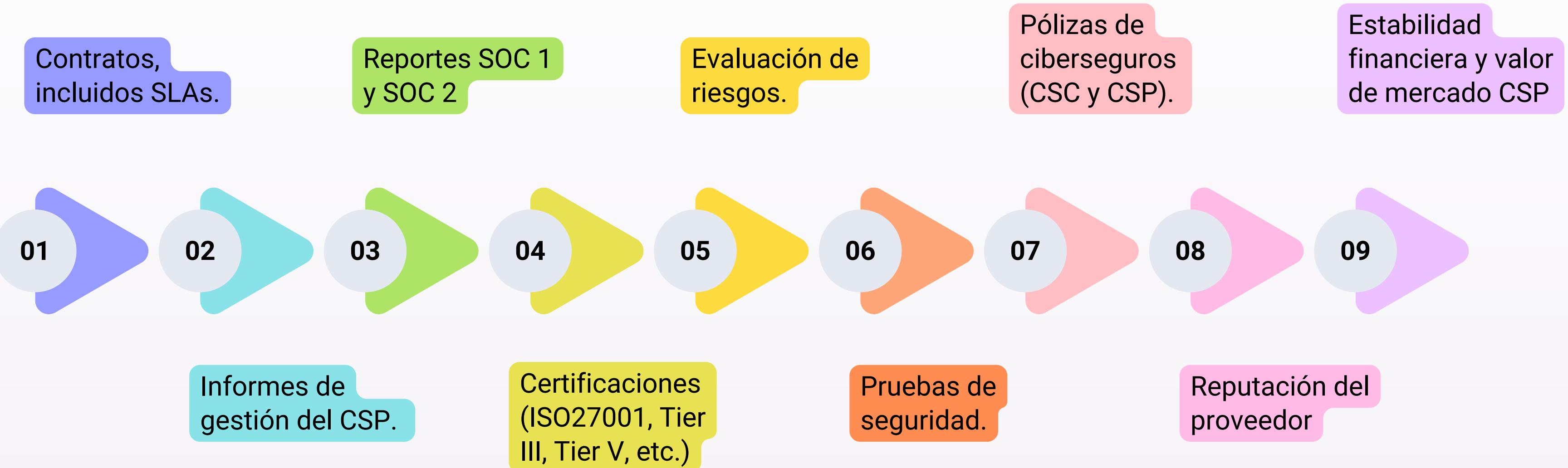


Pregunta lo que quieras

+ Pensando ▾



FUENTES DE ASEGURAMIENTO



REPORTES SOC - SERVICE ORGANIZATION CONTROLS



	OBJETIVO	ALCANCE	DESTINATARIOS
SOC 1	Controles Financieros \$\$\$	Determinado por la organización de servicios	Entidad usuaria y sus auditores.
SOC 2	Controles No Financieros Información	AICPA Trust Services Principles.	Entidad usuaria, sus auditores y otras partes interesadas
SOC 3	Controles No Financieros Información	"Extracto" del SOC 2, de la información no confidencial	Audiencia general.

REPORTES SOC - SERVICE ORGANIZATION CONTROLS

¿Qué información se obtiene de un reporte SOC 2, tipo 2?

Controles de
acceso lógico y
físico

Operaciones del
sistema

Gestión de cambios

Mitigación de
riesgos

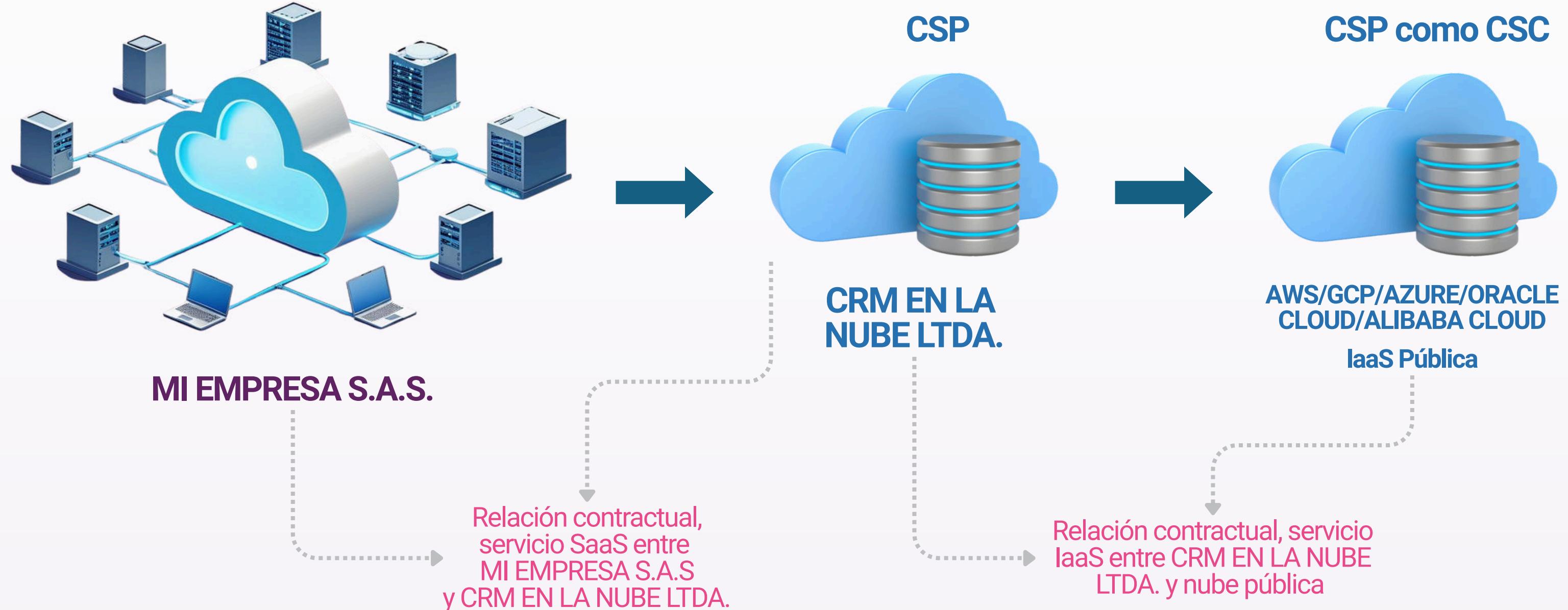
Disponibilidad

Confidencialidad

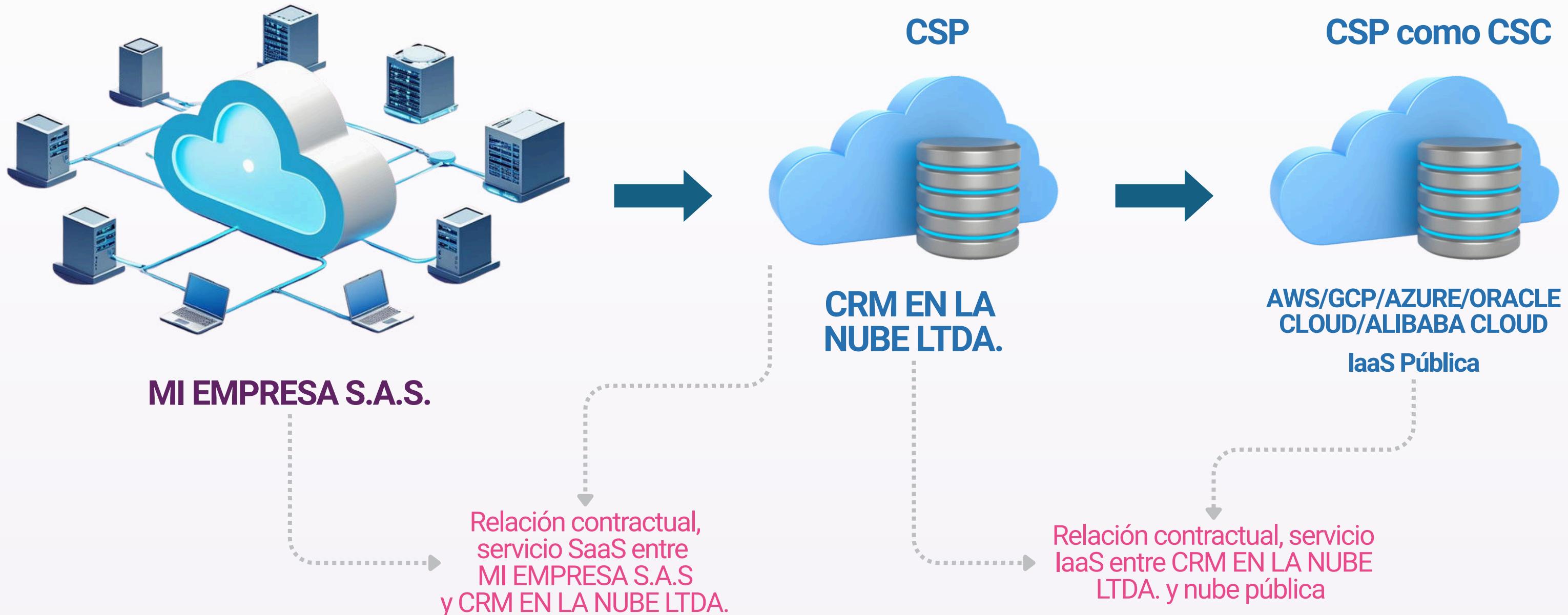
Integridad
procesamiento

Privacidad

REPORTES SOC - SERVICE ORGANIZATION CONTROLS



REPORTES SOC - SERVICE ORGANIZATION CONTROLS



**¿TE ENTREGARON EL REPORTE SOC 2, TIPO 2
DE LA NUBE PÚBLICA?**
(AWS/GCP/AZURE/ORACLE CLOUD/ALIBABA CLOUD)

REPORTES SOC - SERVICE ORGANIZATION CONTROLS





Microsoft Corporation - Microsoft Azure

(Azure & Azure Government)

System and Organization Controls (SOC) 2 Report

July 1, 2018 - June 30, 2019

2
313

^
▼
C
1:1
Q
Q

ChatGPT 5 Thinking ▾

Compartir ...

Microsoft Azure & Azure Government ...
PDF

¡Hola GPT!
Como contexto, se está realizando una auditoría de nube a una compañía Colombiana, del sector financiero, vigilada por la Superintendencia Financiera de Colombia. El archivo adjunto es un reporte SOC 2 Tipo 2 de uno de los proveedores de nube de la empresa.

Resume en 500 palabras máximo lo más relevante de
reporte y si hay algún hallazgo del auditor.

Pensó durante 36s

ChatGPT 5 Thinking

Aquí tienes un resumen ejecutivo del **SOC 2 Tipo II** (Azure & Azure Government) para el período **1-jul-2018 a 30-jun-2019**, enfocado en lo esencial para una entidad financiera supervisada por la SFC:

Alcance y criterios

El examen abarca **Microsoft Azure** (incluyendo **Azure Government**) y la **infraestructura de datacenters** de Microsoft en múltiples ubicaciones globales. Se evaluaron los criterios de **Seguridad, Disponibilidad, Integridad de Procesamiento y Confidencialidad** de los Trust Services Criteria (AICPA), así como controles de CSA CCM v3.0.1 y objetivos BSI C5. El auditor independiente fue **Deloitte & Touche LLP**.

Opinión del auditor

El informe emite **opinión no calificada (unqualified)** sobre el diseño y la efectividad operativa de los controles durante todo el período. **Subservice providers: N/A**. Se registró **1 excepción de prueba** (ver "Hallazgo" abajo).

Compromisos y requisitos del sistema

Azure documenta compromisos de servicio vía **SLA** y acuerdos contractuales (seguridad de datos, disponibilidad/uptime, integridad de procesamiento y confidencialidad), respaldados por políticas y procedimientos operativos y de seguridad corporativos (SBC, SDL, monitoreo y respuesta, auditoría interna).

Cobertura geográfica

Incluye numerosos **datacenters** en EE. UU., Canadá, Europa, Asia–Pacífico, África y Sudamérica (Brasil y Chile, entre otros), relevantes para requisitos de **residencia/ubicación de datos** que suelen aplicar en el sector finaniero.

ChatGPT 5 Thinking

Hallazgo (testing exception)

- Control OA-15 (gestión de contraseñas en dispositivos de red):** El auditor identificó que, en trimestres previos al período actual, **no se retuvo evidencia** para corroborar la **rotación periódica de contraseñas** en dispositivos de red. Al 30-jun-2019 la **remediation seguía en curso**, por lo que **no se realizaron pruebas adicionales de muestras**. **Respuesta de gestión:** Microsoft se compromete a implementar una **solución de rotación automática** de contraseñas para todos los entornos cloud, con **retención de logs**; en tanto, se realizará **rotación manual** donde aún no esté desplegada.

Resultados de control (muestra)

El informe detalla numerosos controles sin excepción (p. ej., **segregación de redes, controles ambientales, clasificación e inventario de activos, gestión y revisión de accesos, MFA / 2FA y políticas de contraseñas/SSPR**), con resultados "**No exceptions noted**" donde aplica.

Responsabilidades del usuario (complementarias)

El informe recuerda responsabilidades del cliente: **cumplimiento normativo, gestión de identidades y contraseñas, revocación de accesos, hardening/patching de componentes propios, planes de DR/BCP, y cifrado** cuando no esté habilitado por defecto. Recomendable mapear estas responsabilidades al **modelo compartido** de tu organización.

Conclusión: Azure obtuvo **opinión limpia** en Seguridad, Disponibilidad, Integridad de Procesamiento y Confidencialidad, con **una excepción puntual** sobre evidencia de rotación de contraseñas en dispositivos de red, en remediation al cierre del período. Esto sugiere un **entorno de control robusto**, con una **área específica a vigilar** en tu evaluación de riesgo de terceros y pruebas continuas.



Certificate of Cloud Auditing Knowledge

The industry's first global cloud auditing credential.



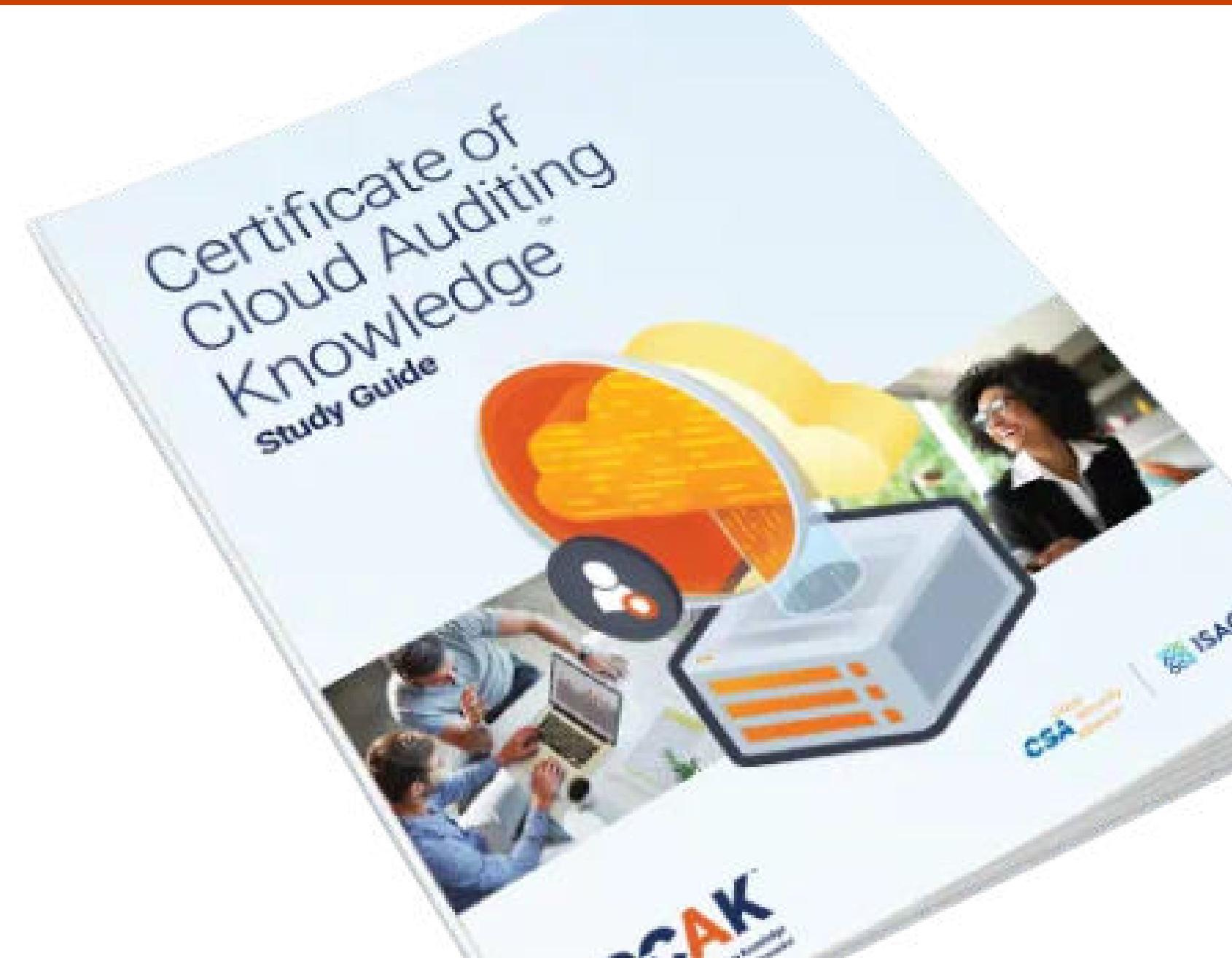
Prepare for the Exam

Qualify for Special Pricing

CCAK™

Certificate of Cloud Auditing Knowledge

A Cloud Security Alliance® and ISACA® Credential



CONCLUSIONES

01

Es crítico identificar el universo de servicios de nube de la organización.

02

Tener claramente identificadas las responsabilidades del CSC y CSP. Contratos.

03

Utilice todas las fuentes de aseguramiento que tenga disponibles.

04

No inventar la rueda, hay marcos, guías, programas ya definidas.

05

Utilicen la IA como apoyo, no como un auditor sin supervisión.



¡MUCHAS GRACIAS!

**FERNEY ANDRÉS
ALVARADO OSPINA**

<https://www.linkedin.com/in/ferneyalvarado/>
ferney@abit-co.com





AteneA

Centro de Pensamiento de Auditoría