CAIGG
CONSEJO DE AUDITORÍA INTERNA GENERAL DE GOBIERNO
Ministerio Secretaría General de la Presidencia

Guía de Auditoría, Seguridad de la Información y Ciberseguridad N°7

COMPUTACIÓN EN LA NUBE

ÍNDICE

Nota

PRESENTACIÓN

En cumplimiento con las instrucciones del Presidente de la República, Gabriel Boric Font, sobre fortalecimiento de la Política de Auditoría Interna de Gobierno; el Consejo de Auditoría Interna General de Gobierno, entidad asesora en materias de auditoría interna, control interno, probidad, gestión de riesgos y gobernanza del Supremo Gobierno, presenta a la Red de Auditoría Gubernamental, la GASIC N°7: Computación en la Nube.

Esta guía es parte de una iniciativa del Consejo de Auditoría Interna General de Gobierno (CAIGG) que busca fortalecer la posición del sector público en materias de Seguridad de la Información y Ciberseguridad, dotando de instrumentos a los Auditores Internos y Servicios Públicos de instrumentos y herramientas que permitan desarrollar un levantamiento de información en base a las mejores prácticas y la legislación vigente.

Santiago, **Junio** 2024.

Daniela Caldana Fulss
Auditora General de Gobierno

Capítulo 1

INTRODUCCIÓN A LA COMPUTACIÓN EN LA NUBE

La computación en la nube es un sistema de computación paralelo y distribuido que consiste en una colección de computadoras interconectadas y virtualizadas, provisionadas dinámicamente y presentadas como uno o más recursos de computación unificados basados en acuerdos de nivel de servicio (SLA) establecidos entre el proveedor y los consumidores. Estos recursos virtualizados pueden reconfigurarse dinámicamente para ajustarse a una carga variable, permitiendo una utilización óptima de los recursos.

La evolución de la computación en la nube se debe al avance de varias tecnologías, especialmente en hardware (virtualización, chips multinúcleo), tecnologías de Internet (servicios web, arquitecturas orientadas a servicios, Web 2.0), computación distribuida (clústeres, grids) y gestión de sistemas (computación autónoma, automatización de centros de datos).

Nota Importante

Estrictamente hablando, **Seguridad de la Información y Ciberseguridad** son dos conceptos diferentes.

La **"Seguridad de la Información"** es la preservación de la Confidencialidad, Integridad y Disponibilidad de la Información en los activos de información, en cualquier medio (incluso, las personas); por otro lado **"Ciberseguridad"** hace referencia exclusiva al ciberespacio y activos digitales.

En esta guía adoptamos el concepto de "Seguridad de la Información y Ciberseguridad", pero para evitar la redundancia y el exceso de texto, utilizaremos los conceptos de "Seguridad de la Información", "Ciberseguridad" o el acrónimo "SIC" como sinónimos para mejorar la comprensión lectora.

1.1 CONCEPTOS ASOCIADOS

Históricamente, la computación ha evolucionado desde el uso de mainframes hasta la computación en la nube actual. Este cambio es comparable a la transición de la generación de energía eléctrica interna a la utilización de una red de suministro de energía. La computación como un servicio de utilidad se define como la entrega bajo demanda de infraestructura, aplicaciones y procesos empresariales en un entorno compartido, escalable y seguro a través de Internet, por una tarifa.

Mashups

La aparición de estándares abiertos de servicios web (WS) ha facilitado la integración de software, permitiendo que las aplicaciones se comuniquen a través de diferentes plataformas de mensajería. La arquitectura orientada a servicios (SOA) empaqueta los recursos de software como "servicios" independientes y bien definidos que pueden ser accedidos de manera uniforme. Los mashups de servicios permiten la combinación programática de información y servicios de diferentes proveedores, creando soluciones complejas a partir de bloques de construcción simples.

Computación en Grida

La computación en grid permite la agregación de recursos distribuidos y su acceso transparente, enfocándose en acelerar aplicaciones científicas como la modelización climática y el análisis de proteínas. La Arquitectura de Servicios Grid Abiertos (OGSA) define capacidades y comportamientos clave para los sistemas grid, promoviendo la estandarización.

Computación como Utilidad

En entornos de computación como utilidad, los usuarios asignan un valor de utilidad a sus trabajos y los proveedores intentan maximizar su propia utilidad (y, por ende, sus beneficios). La computación en nube y la computación como utilidad buscan ofrecer servicios informáticos de manera escalable y bajo demanda.

Virtualización de Hardware

La virtualización de hardware permite ejecutar múltiples sistemas operativos y pilas de software en una única plataforma física. Un monitor de máquina virtual (VMM) o hipervisor gestiona el acceso al hardware físico, presentando a cada sistema operativo invitado una máquina virtual (VM). Las tecnologías innovadoras como los chips multinúcleo y la migración en vivo de VMs han contribuido a la adopción de la virtualización en servidores, mejorando la compartición y utilización de los recursos.

Un aparato virtual es una combinación de una aplicación y el entorno necesario para ejecutarla (sistema operativo, bibliotecas, etc.) Los mercados en línea permiten el intercambio de estos aparatos virtuales, mejorando la personalización, configuración y portabilidad.

Computación Autónoma

La complejidad creciente de los sistemas informáticos ha motivado la investigación en computación autónoma, que busca mejorar los sistemas reduciendo la intervención humana en su operación. Los sistemas autónomos se gestionan a sí mismos con guía humana de alto nivel, apoyándose en sondas de monitoreo, motores de adaptación y efectores para realizar cambios en el sistema.

Migración a la Nube

La migración a la nube presenta oportunidades significativas para las pequeñas y medianas empresas, así como para las grandes corporaciones. Se trata de un modelo disruptivo de IT que combina tecnología y modelo de negocio, permitiendo a las empresas externalizar necesidades de IT no críticas a servicios en la nube. Este modelo ofrece beneficios tanto económicos como tecnológicos, facilitando la adopción de servicios en la nube por parte de empresas de diversos tamaños.

1.2 CONCEPTOS CLAVE

La computación en la nube se refiere a la entrega de servicios de computación a través de Internet. Estos servicios incluyen almacenamiento, procesamiento, bases de datos, redes, software y más. La nube permite a las empresas y usuarios individuales acceder a recursos tecnológicos sin necesidad de invertir en infraestructura física costosa.

Escalabilidad

La capacidad de aumentar o disminuir recursos según la demanda.

Elasticidad

Ajuste automático de recursos para manejar cargas de trabajo variables.

Pago por Uso

Modelo de facturación basado en el consumo real de recursos.

Multi-tenant

Múltiples usuarios comparten los mismos recursos físicos de forma segura y aislada.

1.3 MODELOS DE SERVICIO Y DESPLIEGUE

Existen varios modelos de servicio en la computación en la nube, cada uno con diferentes niveles de control y gestión:

IaaS *(Infraestructura como Servicio)*	Proporciona recursos básicos de computación, almacenamiento y redes. Ejemplos: Amazon EC2, Google Compute Engine.
PaaS *(Plataforma como Servicio)*	Ofrece una plataforma completa para desarrollar, probar y desplegar aplicaciones. Ejemplos: Google App Engine, Microsoft Azure.
SaaS *(Software como Servicio)*	Proporciona aplicaciones listas para usar, accesibles a través de internet. Ejemplos: Google Workspace, Microsoft 365.

Modelos de Despliegue

Nube Pública	Infraestructura compartida y gestionada por un proveedor de servicios de nube, accesible para el público en general.
Nube Privada	Infraestructura dedicada a una sola organización, puede estar gestionada internamente o por un tercero.
Nube Híbrida	Combina nubes públicas y privadas, permitiendo la portabilidad de datos y aplicaciones entre ellas.
Nube Comunitaria	Infraestructura compartida entre varias organizaciones con intereses comunes.

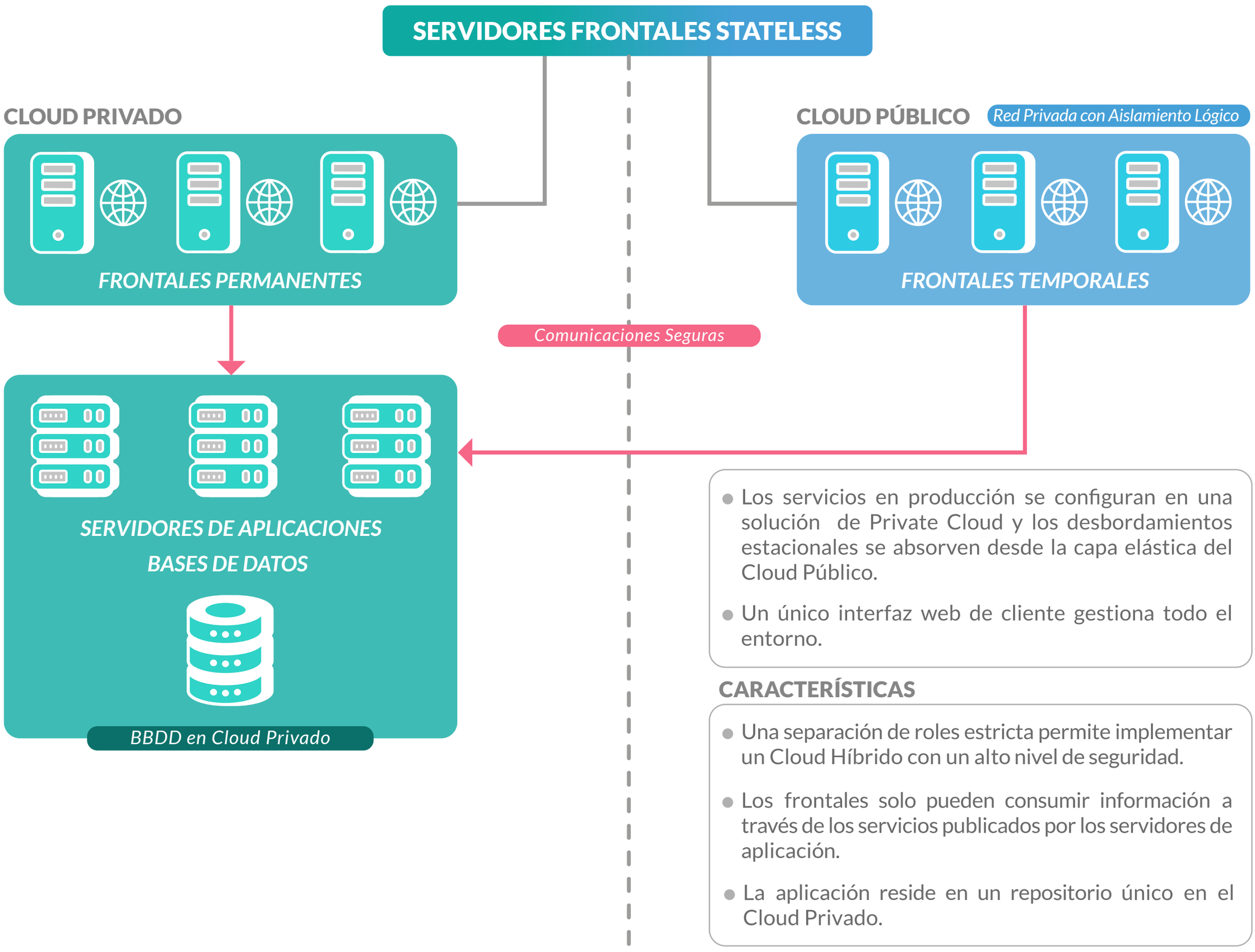


Figura 1. Modelos de Servicio Cloud. Elabroación Propia

1.4 CARACTERÍSTICAS ESENCIALES DE LA NUBE

Las características fundamentales que definen la computación en la nube incluyen:

Acceso a través de la Red

Los servicios de la nube están disponibles a través de Internet, accesibles desde cualquier lugar y dispositivo con conexión a la red.

Elasticidad y Escalabilidad

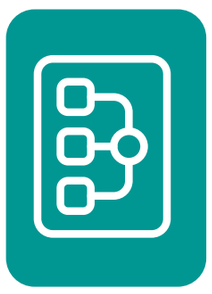
La capacidad que tiene la nube para aumentar o disminuir los recursos de manera automática según las necesidades.

Medición del Servicio

El uso de los recursos de la nube se monitorea, controla y reporta, proporcionando transparencia para el proveedor y el usuario.

Autoservicio Bajo Demanda

Los usuarios pueden aprovisionar y gestionar los recursos de manera autónoma sin necesidad de la intervención del proveedor.



Agrupación de Recursos

Los recursos de la nube están agrupados para servir a múltiples usuarios mediante un modelo multi-tenant, con diferentes recursos asignados dinámicamente según la demanda del usuario.

1.5 VIRTUALIZACIÓN Y SEGURIDAD

La virtualización es una tecnología fundamental en la computación en la nube que permite crear versiones virtuales de recursos físicos, como servidores, almacenamiento y redes. Al abstraer y particionar estos recursos, la virtualización facilita la optimización y gestión eficiente de la infraestructura de TI. Esto permite a las organizaciones consolidar servidores, reducir costos operativos, mejorar la flexibilidad y escalabilidad, y asegurar la continuidad del negocio mediante la migración de máquinas virtuales (VMs) sin interrupciones significativas. A través de herramientas como hipervisores y la virtualización de redes y almacenamiento, se logra una mayor utilización de los recursos disponibles, mejorando la eficiencia y adaptabilidad del entorno tecnológico. Algunos ejemplos de virtualización son: Centros de datos, entornos virtualizados para le desarrollo y prueba de software y escritorios virtuales.

La virtualización trae consigo ciertos beneficios, tales como:

Optimización de Recursos
Permite una mejor utilización del hardware disponible, reduciendo la necesidad de servidores físicos adicionales.

Reducción de Costos
Disminuye los costos operativos y de capital al consolidar servidores y reducir el consumo de energía y espacio físico.

Flexibilidad y Escalabilidad
Facilita la escalabilidad de los recursos de TI y permite una rápida adaptación a cambios en la demanda.

Continuidad del Negocio
Mejora la disponibilidad y la recuperación ante desastres al permitir la migración de VMs entre servidores físicos sin interrupcion.

Tipos de Virtualización

Nº	Tipo de Virtualización	Descripción	Beneficios
01	Virtualización de Servidores	Consiste en particionar un servidor físico en múltiples servidores virtuales, cada uno con su propio sistema operativo y aplicaciones.	Mejora la utilización del hardware, reduce costos de operación y facilita la administración.
02	Virtualización de Almacenamiento	Abstrae los recursos de almacenamiento físico en un grupo de almacenamiento virtual que puede ser gestionado de manera centralizada.	Simplifica la gestión del almacenamiento, mejora la utilización de recursos y facilita el escalamiento.
03	Virtualización de Redes	Permite la creación de redes virtuales independientes sobre una infraestructura de red física, con tecnologías como VLANs y SDN (Software-Defined Networking).	Mejora la flexibilidad y la gestión de la red, permite la segmentación y mejora la seguridad.
04	Virtualización de Escritorios	Permite a los usuarios acceder a un entorno de escritorio completo desde cualquier dispositivo, almacenado y gestionado en un servidor centralizado.	Facilita la administración de escritorios, mejora la seguridad y permite el acceso remoto.

Componentes de la Virtualización

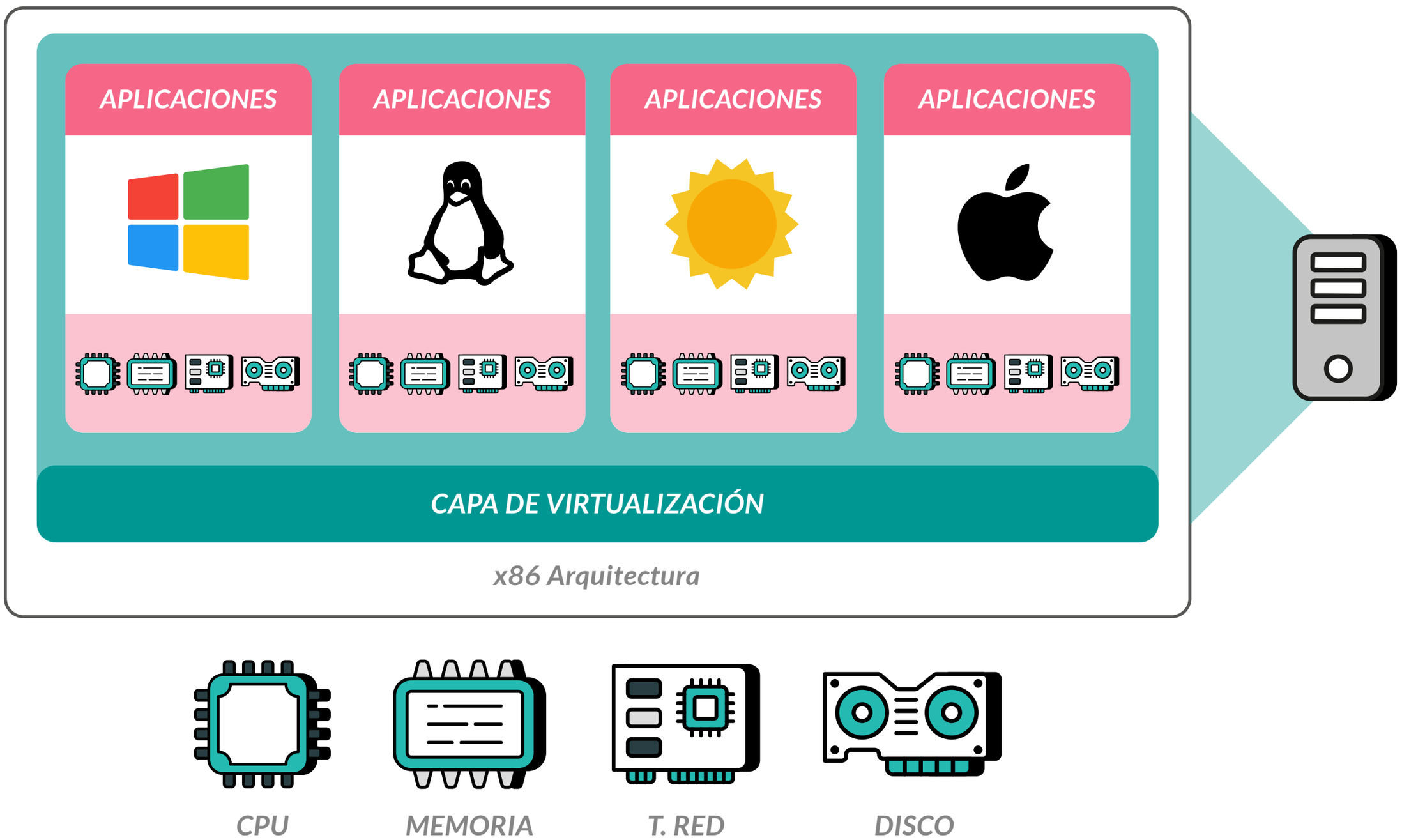


Figura 2. Componentes de la Virtualización. Elabroación Propia.

Hypervisor

Software que permite crear y gestionar máquinas virtuales (VMs). Existen dos tipos:

Tipo 1 - Bare Metal	Corre directamente sobre el hardware del servidor. Ejemplos: VMware ESXi, Microsoft Hyper-V.
Tipo 2 - Hosted	Corre sobre un sistema operativo anfitrión. Ejemplos: VMware Workstation, Oracle VirtualBox.

Máquinas Virtuales (VMs)

Entornos virtuales que operan como computadoras independientes con su propio sistema operativo y aplicaciones.

Gestión de Recursos

Herramientas y software que facilitan la asignación y administración de recursos virtuales, incluyendo CPU, memoria, almacenamiento y red.

Centros de Datos

Utilizan la virtualización para optimizar el uso de recursos y mejorar la eficiencia operativa.

Desarrollo y Pruebas de Software

Facilita la creación de entornos de prueba aislados y la replicación de configuraciones de producción.

Escritorios Virtuales

Permiten a los empleados acceder a sus entornos de trabajo desde cualquier lugar, mejorando la flexibilidad y la productividad.

Capítulo 2

MODELOS DE SERVICIO EN LA NUBE

2.1 MODELOS DE SERVICIO EN LA NUBE

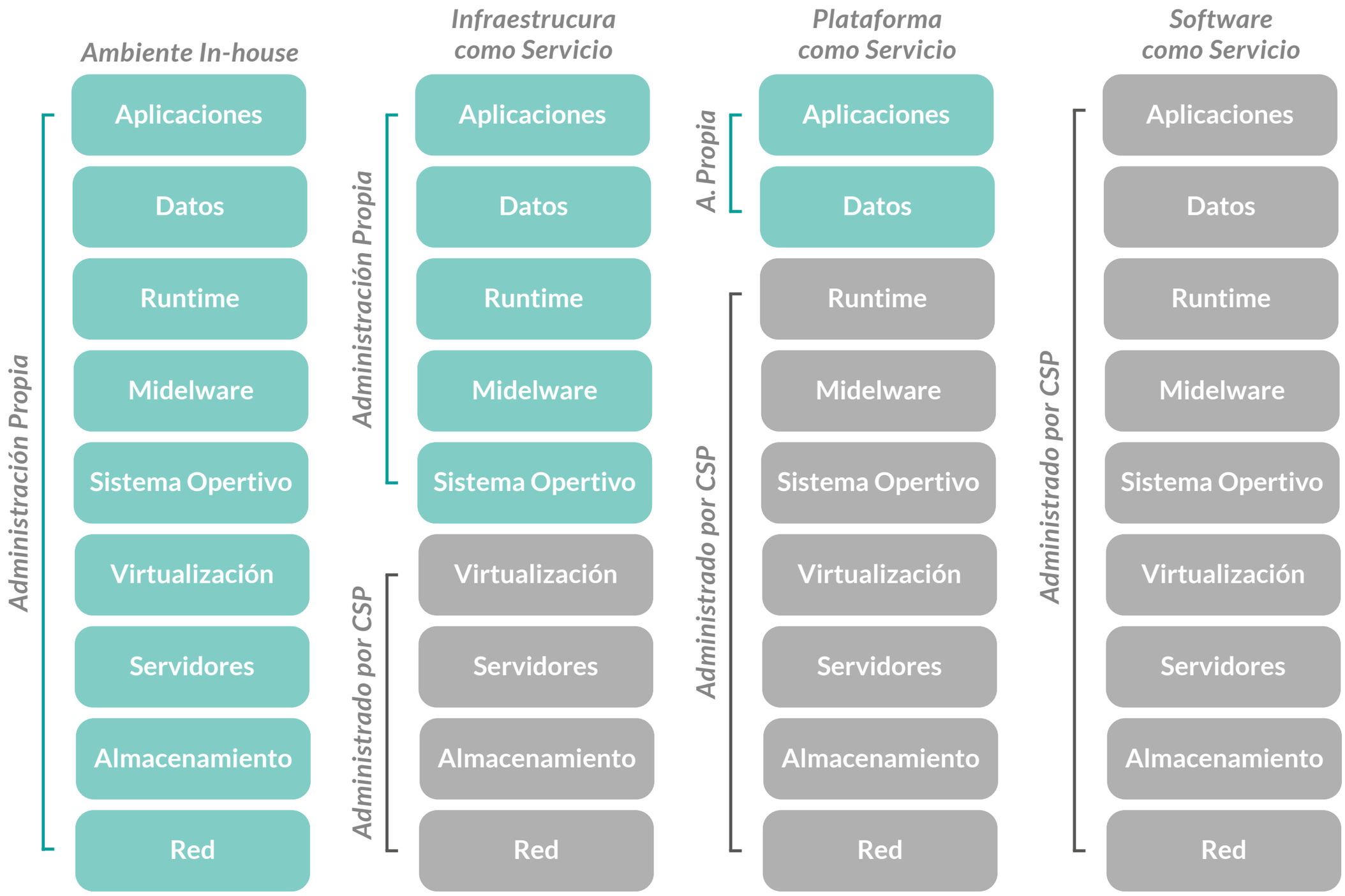


Figura 3. Modelos de Servicio en la Nube. Elabroación Propia.

CSP: Cloud Service Provider

2.2 INFRAESTRUCTURA COMO SERVICIO (IAAS)

Infraestructura como Servicio (IaaS) proporciona recursos informáticos virtualizados a través de Internet. En este modelo, el proveedor de la nube gestiona la infraestructura física, mientras que los usuarios administran el sistema operativo, las aplicaciones y los datos.

Características Clave:

01 **Recursos Virtualizados**
Incluye máquinas virtuales, almacenamiento, redes y otros recursos informáticos.

02 **Flexibilidad y Control**
Los usuarios tienen un alto grado de control sobre el sistema operativo y las aplicaciones instaladas.

03 **Escalabilidad**
Los recursos pueden escalarse hacia arriba o hacia abajo según las necesidades del usuario.

04 **Pago por Uso**
Los usuarios pagan solo por los recursos que utilizan, lo que puede incluir el tiempo de uso de máquinas virtuales, almacenamiento y ancho de banda.

Ventajas:

01 **Costos Reducidos**
Elimina la necesidad de invertir en infraestructura física.

02 **Rapidez de Implementación**
Permite la rápida provisión de recursos según sea necesario.

03 **Flexibilidad**
Ofrece un entorno altamente flexible que puede adaptarse a diferentes necesidades empresariales.

Ejemplos de Proveedores de IaaS

- Amazon Web Services (AWS) EC2
- Google Compute Engine (GCE)
- Microsoft Azure Virtual Machines

2.3 PLATAFORMA COMO SERVICIO (PAAS)

Plataforma como Servicio (PaaS) proporciona una plataforma que permite a los desarrolladores crear, desplegar y gestionar aplicaciones sin preocuparse por la infraestructura subyacente. PaaS incluye herramientas de desarrollo, bases de datos, servicios de integración y más.

Características Clave:

01 **Entorno de Desarrollo Integrado**
Proporciona todas las herramientas necesarias para el desarrollo de aplicaciones.

02 **Automatización de Tareas**
Tareas como el aprovisionamiento de servidores, almacenamiento y redes están automatizadas.

03 **Escalabilidad**
Las aplicaciones pueden escalarse automáticamente en función de la demanda.

04 **Gestión Simplificada**
El proveedor se encarga del mantenimiento de la infraestructura y las actualizaciones de software.

Ventajas:

01 **Mayor Productividad**
Facilita el desarrollo y despliegue rápido de aplicaciones.

02 **Reducción de Costos**
Los desarrolladores pueden centrarse en el código sin preocuparse por la gestión de la infraestructura.

03 **Innovación Rápida**
Permite la adopción rápida de nuevas tecnologías y servicios.

Ejemplos de Proveedores de PaaS

- Google App Engine
- Microsoft Azure App Services
- Heroku

2.4 SOFTWARE COMO SERVICIO (SAAS)

Software como Servicio (SaaS) ofrece aplicaciones listas para usar que son accesibles a través de Internet. Los usuarios finales pueden acceder a las aplicaciones a través de un navegador web, sin necesidad de instalar software en sus dispositivos locales.

Características Clave:

01 **Accesibilidad**
Las aplicaciones están disponibles desde cualquier lugar con conexión a Internet.

02 **Mantenimiento**
El proveedor se encarga de la gestión y mantenimiento del software, incluyendo actualizaciones y parches de seguridad.

03 **Modelos de Suscripción**
Los usuarios generalmente pagan una tarifa de suscripción mensual o anual.

04 **Escalabilidad**
Los servicios SaaS pueden escalarse fácilmente para adaptarse a un mayor número de usuarios o un aumento en la demanda de recursos.

Ventajas:

01 **Facilidad de Uso**
No se requiere instalación ni mantenimiento por parte del usuario.

02 **Ahorro de Costos**
Elimina la necesidad de comprar y mantener hardware y software.

03 **Actualizaciones Automáticas**
Los usuarios siempre tienen acceso a la versión más reciente del software.

Capítulo 3

SEGURIDAD EN LA NUBE

3.1 CONCEPTOS Y DEFINICIONES

La seguridad en la nube implica proteger datos, aplicaciones e infraestructuras asociadas a la computación en la nube. Esto abarca desde la protección de datos en tránsito y en reposo, hasta el control de acceso y la seguridad de las aplicaciones.

Conceptos Clave

- **Confidencialidad:** Garantizar que la información solo sea accesible a personas autorizadas.
- **Integridad:** Asegurar que los datos no sean alterados o eliminados sin autorización.
- **Disponibilidad:** Asegurar que los servicios y datos estén disponibles cuando se necesiten.
- **Autenticación:** Verificar la identidad de los usuarios y sistemas que acceden a los recursos.
- **Autorización:** Controlar qué recursos pueden ser accedidos por usuarios autenticados.
- **Auditoría:** Monitorear y registrar las actividades para detectar y responder a incidentes de seguridad.

3.2 MODELOS DE RESPONSABILIDAD DE SEGURIDAD

La seguridad en la nube se gestiona mediante un modelo de responsabilidad compartida entre el proveedor de servicios en la nube y el cliente.

Ejemplos de Modelos de Responsabilidad Compartida

Modelo	*Ejemplo*
IaaS	El proveedor se encarga de la seguridad de la infraestructura física, mientras que el cliente gestiona la seguridad del sistema operativo, las aplicaciones y los datos. .
PaaS	El proveedor gestiona la seguridad del entorno de desarrollo, mientras que el cliente es responsable de la seguridad de las aplicaciones que desarrolla.
SaaS	El proveedor se encarga de la seguridad de la aplicación y los datos subyacentes, mientras que el cliente debe gestionar el acceso y la configuración de usuario.

3.3 CONTROLES DE SEGURIDAD

Implementar controles de seguridad es esencial para proteger los recursos en la nube. Estos controles incluyen medidas técnicas, políticas y procedimientos.

Controles Técnicos

Cifrado de Datos	Protege los datos en tránsito y en reposo mediante técnicas de cifrado.
Control de Acceso	Utiliza autenticación multifactor (MFA) y políticas de acceso basadas en roles (RBAC).
Monitoreo y Detección	Herramientas de monitoreo continuo y detección de intrusos para identificar y responder a amenazas.
Seguridad de Redes	Implementa firewalls, segmentación de redes y VPNs para proteger el tráfico de red.

Controles Administrativos

Políticas de Seguridad	Establece políticas de seguridad claras y detalladas para los usuarios y administradores.
Capacitación	Proporciona formación regular en seguridad a todos los empleados.
Gestión de Incidentes	Planes y procedimientos para la gestión y respuesta a incidentes de seguridad.

Controles Físicos

Seguridad de Centros de Datos	Implementa medidas de seguridad física en los centros de datos, como control de acceso, vigilancia y protección contra desastres naturales.
Protección de Hardware	Asegura el hardware utilizado para la infraestructura de la nube.

Buenas Prácticas

Evaluación de Riesgos	Realiza evaluaciones de riesgo periódicas para identificar y mitigar vulnerabilidades.
Actualizaciones y Parcheo	Mantén todos los sistemas y aplicaciones actualizados con los últimos parches de seguridad.
Auditoría y Cumplimiento	Realiza auditorías regulares para asegurar el cumplimiento de las políticas de seguridad y normativas aplicables.

Capítulo 4

GOBIERNO DE LA INFORMACIÓN EN LA NUBE

4.1 CLASIFICACIÓN Y POLÍTICAS DE GESTIÓN DE LA INFORMACIÓN

El gobierno de la información en la nube se refiere a las políticas y prácticas utilizadas para gestionar la seguridad, la privacidad y el cumplimiento de los datos almacenados y procesados en la nube. El gobierno de la ciberseguridad, cuando se refiere a la computación en la nube, tiene como responsabilidad definir la forma en la que la organización entiende los conceptos típicos en datos, por ejemplo, la definición de los criterios para la clasificación de la información, A demás, dirigir la operación y procesos de la seguridad en la nube a través de políticas, recursos y roles.

Clasificación de la Información

- **Sensibilidad:** Clasificar los datos según su sensibilidad. (Por ejemplo: datos públicos, confidenciales, alta confidencialidad).
- **Valor:** Determinar el valor de los datos para la organización y establecer medidas de protección adecuadas.
- **Ciclo de Vida:** Identificar las etapas del ciclo de vida de los datos. (Creación, almacenamiento, uso, archivo, destrucción).

Políticas de Gestión de la Información

- **Política de Uso de Datos:** Define cómo se deben manejar y utilizar los datos dentro de la organización.
- **Política de Retención de Datos:** Especifica cuánto tiempo deben conservarse los datos y cuándo deben eliminarse.
- **Política de Seguridad de Datos:** Establece las medidas de seguridad necesarias para proteger los datos contra accesos no autorizados y brechas de seguridad.

4.2 ROLES Y RESPONSABILIDADES PARA LA PROPIEDAD Y CUSTODIA DE DATOS

La propiedad y custodia de los datos en la nube implican la asignación de responsabilidades para la gestión y protección de los datos.
Esto incluye la definición de roles específicos para la gestión de datos, como custodio de datos o comprender el rol de propietario de los datos.

Propietario de los Datos

- **Definición:** Puede ser un departamento, una unidad de negocio o una persona dentro de la organización.
- **Responsabilidades:** El propietario de los datos es responsable de la exactitud, integridad y protección de los datos. Debe definir quién tiene acceso a los datos y qué niveles de acceso son apropiados.

Custodio de los Datos

- **Definición:** El custodio de los datos es responsable de la implementación técnica de las políticas y controles de seguridad definidos por el propietario de los datos.
- **Responsabilidades:** **El custodio de los datos es responsable de que se cumpla con los controles y estándares establecidos.**

4.3 CICLO DE VIDA DE LA SEGURIDAD DE LOS DATOS

El ciclo de vida de la seguridad de los datos abarca todas las etapas desde la creación hasta la destrucción de los datos, asegurando que se apliquen controles de seguridad adecuados en cada etapa.

Etapas del Ciclo de Vida de los Datos

01	Etapa de Creación	Generación de nuevos datos o captura de datos existentes.
	Control de Seguridad	Aplicar cifrado en la creación de datos sensibles.
02	Etapa de Almacenamiento	Guardar datos en repositorios seguros.
	Control de Seguridad	Implementar cifrado en reposo y controles de acceso para proteger los datos almacenados.
03	Etapa de Uso	Acceso y procesamiento de datos por usuarios autorizados.
	Control de Seguridad	Utilizar autenticación multifactor (MFA) y políticas de acceso basadas en roles (RBAC).
04	Etapa de Compartir	Distribuir datos a usuarios internos o externos.
	Control de Seguridad	Aplicar cifrado en tránsito y asegurar que solo usuarios autorizados puedan acceder a los datos compartidos.
05	Etapa de Archivar	Mover datos a almacenamiento de largo plazo cuando ya no se utilizan activamente.
	Control de Seguridad	Asegurar que los datos archivados estén cifrados y accesibles solo a usuarios autorizados.
06	Etapa de Destrucción	Eliminación segura de datos cuando ya no sean necesarios.
	Control de Seguridad	Utilizar métodos de eliminación segura, como el borrado seguro o la destrucción física de medios de almacenamiento.

Buenas Prácticas

- **Auditoría y Monitoreo:** Realizar auditorías regulares y monitorear el acceso y uso de los datos para detectar y responder a incidentes de seguridad.
- **Cumplimiento Normativo:** Asegurarse de que las políticas y prácticas de gestión de datos cumplan con las regulaciones y estándares de la industria, como GDPR, HIPAA, etc.
- **Educación y Capacitación:** Proporcionar capacitación continua a los empleados sobre las políticas de gestión de la información y las mejores prácticas de seguridad.

Capítulo 5

PROTECCIÓN DE DATOS EN LA NUBE

5.1 PREVENCIÓN DE FUGA DE DATOS (DLP)

La prevención de fuga de datos (Data Loss Prevention, DLP) es una estrategia para asegurar que los datos sensibles no sean accidental o intencionalmente divulgados fuera de la organización.

Elementos Clave de DLP

Monitoreo
Vigilancia continua del flujo de datos dentro y fuera de la organización.

Identificación de Datos Sensibles
Utilizar técnicas de reconocimiento para identificar y clasificar datos sensibles.

Políticas de Control
Establecer y aplicar políticas para el manejo y transferencia de datos sensibles.

Alertas y Acciones
Configurar alertas y acciones automatizadas cuando se detecten violaciones de políticas de datos.

Ejemplos de Soluciones DLP

Google Cloud DLP: Proporciona capacidades para identificar, clasificar y proteger datos sensibles.

Microsoft Azure Information Protection: Clasificación, etiquetado y protección de documentos y correos electrónicos.

Buenas Prácticas en DLP

Capacitación
Educar a los empleados sobre la importancia de proteger los datos sensibles y cómo seguir las políticas de DLP.

Integración con CASB
Utilizar Cloud Access Security Brokers (CASB) para extender las capacidades de DLP a entornos de nube.

Auditoría y Revisión
Realizar auditorías periódicas para revisar y mejorar las políticas y prácticas de DLP.

5.2 GESTIÓN DE IDENTIDADES Y ACCESOS

La gestión de identidades y accesos (IAM) es fundamental para asegurar que solo las personas autorizadas puedan acceder a los recursos y datos en la nube. Para más detalles ver GASIC N°3 "Gestión de Identidad y Accesos".

Elementos Clave de IAM

- **Autenticación:** Verificación de la identidad de los usuarios, con métodos como contraseñas, biometría, y autenticación multifactor.
- **Autorización:** Definición de permisos y políticas que determinan qué recursos y datos pueden ser accedidos por cada usuario.
- **Gestión de Roles:** Asignación de roles a usuarios con permisos específicos según su función dentro de la organización.
- **Federación de Identidades:** Permite el uso de identidades externas para acceder a los recursos internos de la nube.

Estándares de IAM

- **SAML (Security Assertion Markup Language):** Protocolo estándar para autenticación y autorización de usuarios entre diferentes dominios de seguridad.
- **OAuth:** Protocolo estándar para autorización que permite el acceso a los recursos del usuario sin compartir las credenciales.
- **OpenID Connect:** Extensión de OAuth 2.0 para autenticación de usuarios.

Buenas Prácticas en IAM

- **Principio de Menor Privilegio:** Otorgar a los usuarios el nivel mínimo de acceso necesario para realizar sus tareas.
- **Revisión Periódica de Accesos:** Realizar revisiones regulares de los accesos y permisos para asegurar que estén actualizados y sean necesarios.
- **Autenticación Multifactor:** Implementar MFA para todas las cuentas, especialmente las que tienen acceso privilegiado.

Capítulo 6

CUMPLIMIENTO Y AUDITORÍAS EN LA NUBE

6.1 IMPACTO DE LA NUBE EN EL CUMPLIMIENTO LEGAL

El uso de servicios en la nube introduce nuevas consideraciones para el cumplimiento legal, ya que los datos y servicios pueden estar distribuidos en múltiples ubicaciones geográficas y administrados por terceros. Es crucial entender cómo la nube afecta las obligaciones legales y los requisitos regulatorios.

Aspectos Clave

- **Jurisdicción:** La ubicación física de los datos puede afectar las leyes aplicables. Es importante saber dónde se almacenan los datos y cuáles son las leyes locales de protección de datos.
- **Transferencia de Datos:** Las transferencias de datos transfronterizas deben cumplir con las regulaciones internacionales, como el Reglamento General de Protección de Datos (GDPR) en Europa.
- **Responsabilidades Compartidas:** Entender el modelo de responsabilidad compartida y cómo se distribuyen las responsabilidades de cumplimiento entre el proveedor de servicios en la nube y el cliente.

Buenas Prácticas

- **Evaluar las Leyes Locales:** Realizar un análisis exhaustivo de las leyes y regulaciones aplicables en todas las jurisdicciones donde se almacenan o procesan los datos.
- **Contratos Claros:** Asegurar que los contratos con los proveedores de servicios en la nube especifican claramente las responsabilidades de cumplimiento.
- **Auditorías y Certificaciones:** Optar por proveedores que posean certificaciones reconocidas (como ISO 27001, SOC 2) y realizar auditorías regulares.

6.2 AUDITORÍA EN LA NUBE

Las auditorías en la nube son esenciales para verificar que los proveedores de servicios cumplen con los requisitos de seguridad y cumplimiento. Estas auditorías pueden ser realizadas por el propio proveedor, por terceros o por el cliente.

Tipos de Auditorías

Auditorías Internas	Realizadas por el equipo interno del proveedor de servicios para asegurar que se siguen las políticas y procedimientos.
Auditorías Externas	Realizadas por auditores independientes para validar el cumplimiento de estándares y regulaciones.
Auditorías del Cliente	Los clientes pueden realizar auditorías para asegurar que el proveedor cumple con sus requisitos específicos de seguridad y cumplimiento.

Elementos a Auditar

- **Seguridad de Datos:** Evaluar cómo se protegen los datos en tránsito y en reposo.
- **Control de Acceso:** Verificar que existen controles adecuados para gestionar y monitorear el acceso a los recursos y datos.
- **Cumplimiento Normativo:** Asegurar que se cumplen con todas las regulaciones aplicables.
- **Disponibilidad y Resiliencia:** Revisar las medidas implementadas para garantizar la disponibilidad y recuperación ante desastres.

Elementos a Auditar

- **Seguridad de Datos:** Evaluar cómo se protegen los datos en tránsito y en reposo.
- **Control de Acceso:** Verificar que existen controles adecuados para gestionar y monitorear el acceso a los recursos y datos.
- **Cumplimiento Normativo:** Asegurar que se cumplen con todas las regulaciones aplicables.
- **Disponibilidad y Resiliencia:** Revisar las medidas implementadas para garantizar la disponibilidad y recuperación ante desastres.

Herramientas y Métodos

Revisiones de Políticas y Procedimientos	Examinar la documentación de políticas y procedimientos del proveedor.
Pruebas de Seguridad	Realizar pruebas de penetración y evaluaciones de vulnerabilidad.
Monitoreo y Reportes	Utilizar herramientas de monitoreo continuo y revisar los reportes de seguridad y cumplimiento.

6.3 COORDINACIÓN CON REGULADORES

La colaboración con los reguladores es crucial para asegurar el cumplimiento de las normativas y para mantenerse actualizado con los cambios en las leyes y regulaciones.

Pasos Clave

01	Comunicación Continua	Mantener una comunicación abierta y continua con los reguladores para entender las expectativas y requisitos.
02	Participación en Foros y Grupos de Trabajo	Involucrarse en foros y grupos de trabajo relacionados con la regulación de la nube para mantenerse informado sobre las mejores prácticas y cambios normativos.
03	Reportes Regulares	Proveer reportes regulares a los reguladores sobre el estado de cumplimiento y cualquier incidente relevante.

Ejemplos de Regulaciones

- **GDPR (Reglamento General de Protección de Datos):** Regula la protección de datos personales en la Unión Europea.
- **HIPAA (Health Insurance Portability and Accountability Act):** Regula la protección de información de salud en E.E.U.U.
- **CCPA (California Consumer Privacy Act):** Regula la privacidad de los datos de los consumidores en California, EE. UU.

6.4 ROL DEL AUDITOR PÚBLICO GUBERNAMENTAL

El auditor público gubernamental juega un papel crucial en la supervisión del cumplimiento y la seguridad de los servicios en la nube utilizados por las entidades gubernamentales. Este rol incluye evaluar la conformidad con las leyes, regulaciones y políticas aplicables.

Responsabilidades

Evaluación de Cumplimiento	Verificar que las entidades gubernamentales cumplen con las normativas y políticas de seguridad de la información.
Revisión de Contratos	Asegurar que los contratos con proveedores de servicios en la nube incluyen cláusulas adecuadas de seguridad y cumplimiento.
Monitoreo Continuo	Implementar un sistema de monitoreo continuo para detectar y responder a incidentes de seguridad.

Buenas Prácticas

Auditorías Regulares	Realizar auditorías periódicas y revisiones de cumplimiento para identificar y mitigar riesgos.
Capacitación Continua	Mantener al personal actualizado con las últimas regulaciones y prácticas de seguridad.
Colaboración con Proveedores	Trabajar estrechamente con los proveedores de servicios en la nube para asegurar una implementación segura y conforme.

Capítulo 7

USO DE LA GUÍA PARA LA AUDITORÍA INTERNA

7.1 CÓMO UTILIZAR LA GUÍA PARA LA AUDITORÍA INTERNA

Para que el auditor interno pueda aprovechar al máximo esta publicación, es conveniente que se refiera a los instrumentos complementarios: Las preguntas de auditoría temáticas y el modelo de madurez general. Cada GASIC se compone de tres componentes:

Guía de Auditoría de la Seguridad de la Información y Ciberseguridad (GASIC):
Este es el cuerpo teórico y consiste en el marco contextual necesario para que el auditor interno comprenda el alcance y del dominio de seguridad que está evaluando. Es un instrumento con los conceptos fundamentales recopilados de mejores prácticas.

Modelo de Madurez:
Recopila controles desde las mejores prácticas asociadas al tema central de Guía de Auditoría, organiza los controles en una propuesta de madurez y permite al auditor conocer los requisitos que debería evaluar.

Ejemplos de Preguntas de Auditoría:
Complementa el modelo de madurez a través de una serie de preguntas organizadas en varios documentos. Cada documento representa un control que pertenece a uno de los ejes temáticos definidos al interior de la Guía de Auditoría.

La ilustración a continuación presenta esta estructura documental:

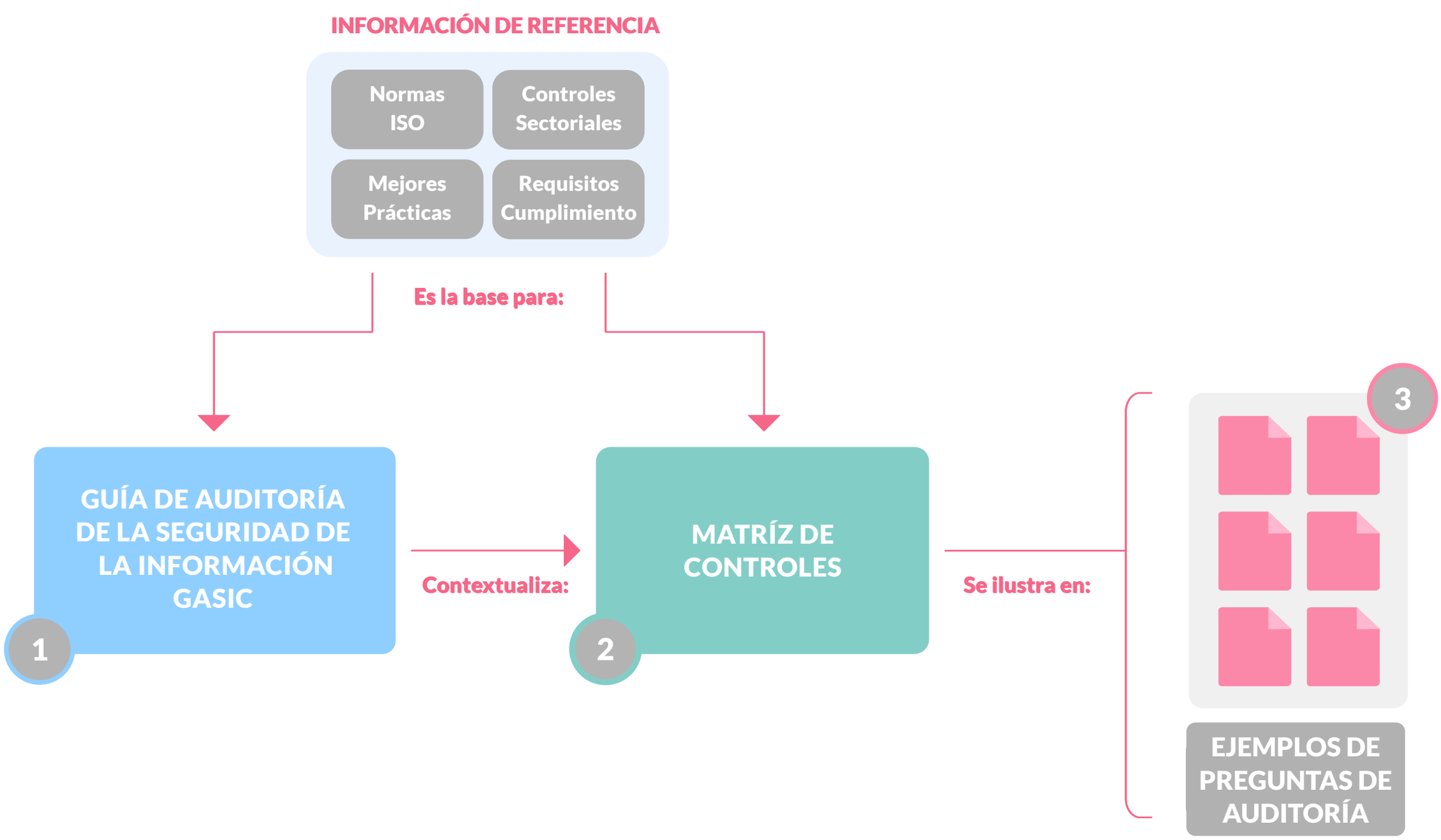


Figura 4. Modo de uso y Estructura Documental GASIC.

El método de trabajo sugerido es el siguiente:

01 **El auditor interno debe estudiar cada Guía de Auditoría y su contexto para tener plena comprensión del tema a trabajar.**

02 **A continuación, puede utilizar el Modelo de Madurez para seleccionar los controles que sean apropiados para la organización. La selección de controles debe estar alineados con:**

- **a. La estrategia de la organización.**
- **b. Los resultados de la evaluación de riesgos.**
- **c. Los requisitos de cumplimiento.**
- **d. La estrategia de auditoría interna, expresada en el plan.**

03 **Por último, puede utilizar los documentos de ejemplo para la planificación de las preguntas y pruebas que fuese a realizar. El formato del programa, plan, instrumentos, pruebas y reportería debe ser aquel solicitado en el contexto de cada auditoría, que está fuera del alcance de esta guía.**

NOTA

Los ejemplos de pruebas tienen como propósito ilustrar la forma en la que los requisitos de los marcos que se encuentran en el matriz de controles. El auditor puede elegir utilizar un conjunto de estos ejemplos o diseñar sus propias pruebas para evaluar el nivel de cumplimiento de cada control.

En ningun caso, los ejemplos pretenden ser una lista completa; recuerde, debe contextualizar el ejercicio a la realidad de su organización.

Ejes temáticos

1. Gobierno y Cumplimiento en Nube: Este eje temático se enfoca en gestionar auditorías, seguridad y cumplimiento, asegurando controles claros y monitoreo continuo. También incluye aspectos legales y regulatorios, estableciendo alineación con normas y estándares aplicables. Se resaltan políticas de seguridad para la nube, con medidas para acceso, respaldo y acuerdos con proveedores, junto con la gestión de riesgos mediante controles criptográficos y administración de claves

	OBJETIVO ESPECÍFICO	CRITERIO DE AUDITORÍA
1	**Auditoría y Monitoreo**	**La organización debe gestionar auditorías, seguridad y cumplimiento en la nube con controles claros, inventarios actualizados, monitoreo, gestión de incidentes y verificación de controles, definiendo responsabilidades y abordando brechas de cumplimiento para**
2	**Legal y Regulatorio**	**La organización debe identificar las autoridades pertinentes y las funciones de seguridad asociadas al servicio en la nube, como respaldo, controles criptográficos y gestión de incidentes. Debe garantizar el cumplimiento de licencias, regulaciones y acuerdos internacionales, implementando controles y pruebas periódicas**
3	**Politicas Asociadas a la Nube**	**La organización debe establecer políticas de seguridad de la información para la nube, asegurando el cumplimiento de normativas y niveles aceptables de riesgo. Estas políticas deben incluir restricciones al acceso, respaldo de datos, medidas disciplinarias y acuerdos claros con proveedores para garantizar la seguridad y disponibilidad de los sistemas. Además, deben revisarse periódicamente para garantizar su eficacia y alineación con la legislación aplicable.**
4	**Riesgos en la Nube**	**La organización debe gestionar claves criptográficas en la nube, implementar controles de seguridad para mitigar riesgos y revisar capacidades criptográficas del proveedor para cumplir con las políticas internas. Debe garantizar la administración de claves por el cliente cuando corresponda, documentar procedimientos**

2. Seguridad y Protección en la Nube: Este eje temático tiene como objetivo el control de acceso mediante requisitos claros, autentificación y gestión de registros de usuarios. Incluye lineamientos para operaciones seguras, como la gestión de eventos, respaldo, recuperación y monitoreo de capacidad. Además, se destaca la protección de datos mediante cifrado, restricciones en entornos de prueba y medidas para asegurar la integridad y recuperación de la información.

	OBJETIVO ESPECÍFICO	CRITERIO DE AUDITORÍA
1	**Control de Acceso a la Nube**	**La organización debe establecer requisitos claros para el acceso de los usuarios a servicios en la nube, verificar que los proveedores cumplan con procedimientos adecuados de autenticación y asignación de información secreta, y gestionar de manera oportuna los registros, bajas y cambios de acceso de usuarios.**
2	**Operaciones en la Nube**	**La organización debe acordar roles y responsabilidades de seguridad con el proveedor de servicios en la nube, garantizar la capacidad necesaria y establecer mecanismos para la gestión de eventos de seguridad y copias de respaldo. También debe evaluar el impacto de interrupciones, priorizar la recuperación de servicios críticos, monitorear la capacidad de la nube y planificar transferencias a proveedores alternativos si es necesario. Finalmente, debe realizar evaluaciones de riesgos regulares y fomentar una cultura de seguridad cibernética para mejorar continuamente los controles frente a nuevas amenazas.**
3	**Proteccion de datos en la Nube**	**La organización debe implementar rutinas de integridad para el manejo de datos, cifrar datos en tránsito y almacenados, y prohibir el uso de copias de producción en entornos de prueba. Además, debe garantizar la capacidad de respaldo y recuperación, proteger almacenes de claves y limitar el acceso a funciones críticas.**