ISACA Quito Chapter

GESTIÓN DE SERVICIOS EN LA NUBE

Juan Carlos López, CISA, CISM, CRISC, CGEIT, PMP
+593 995061566
https://www.linkedin.com/in/jclopezexacta/


20 de junio de 2024


9:00


Virtual

Evento exclusivo para la SEPS

ISACA®

Quito Chapter

Empezamos en unos minutos

ISACA Quito Chapter

GESTIÓN DE SERVICIOS EN LA NUBE

Juan Carlos López

Consultor con experiencia en definición, implementación y gestión de prácticas de gobierno, administración de riesgos, control interno planeación estratégica, auditoria y dirección de proyectos; del negocio y tecnología. Durante 5 años fue consultor de PricewaterhouseCoopers. Fue Gerente de Auditoría, de Tecnología y de la Oficina de Dirección de Proyectos del Banco Internacional, durante los ocho años que laboró en la Institución. Miembro de asociaciones profesionales como el Instituto de Dirección de Proyectos (PMI), de la Asociación para la Auditoría y Control de Sistemas de Información (ISACA) y del Instituto para la Gobernabilidad de Tecnología de Información (ITGI), de estos dos últimos fue Presidente y Director de Educación. Posee las Certificaciones CISA, CISM, CRISC, CGEIT, SMC, PMP, ITIL y COBIT. Es instructor COBIT 2019 acreditado por APMG. Docente en la Universidad de la Américas en las maestrías de Gerencia de Sistemas, Gerencia de Seguridad de la Información y Gerencia de Operaciones en las asignaturas de Gobierno de Información & Tecnología, Gobierno de Seguridad de la Información y Dirección de Proyectos.

.aspx

+593 995061566
https://www.linkedin.com/in/jclopezexacta/

ISACA

Conceptualización de la Nube: Perspectivas de NIST e ISO/IEC

NIST define la computación en la nube como:

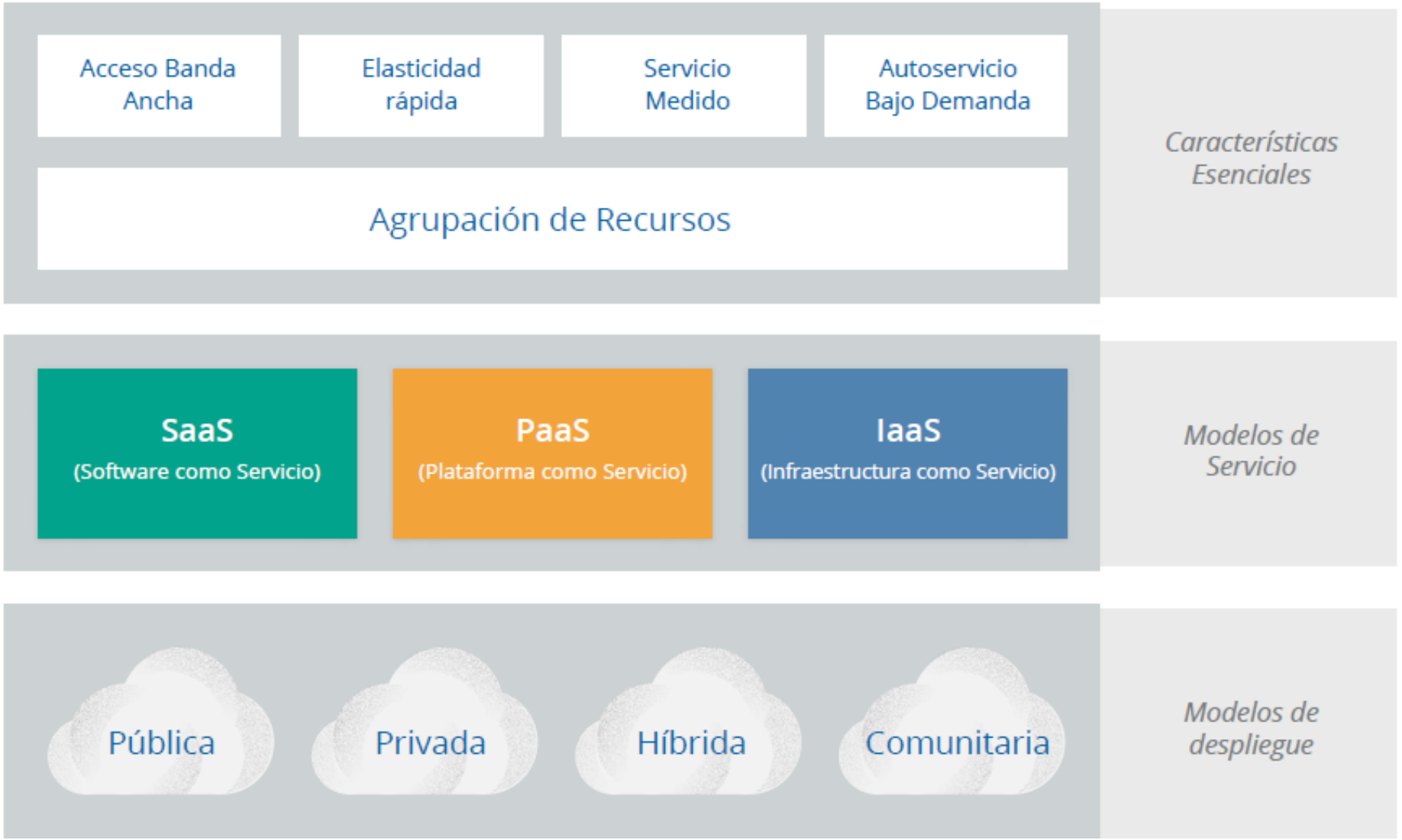
La computación en la nube es un modelo para permitir un acceso de red ubicuo, conveniente y bajo demanda a un grupo compartido de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que pueden aprovisionarse y liberarse rápidamente con un mínimo esfuerzo o interacción del proveedor de servicio.

La definición de ISO/IEC es muy similar:

Paradigma para permitir el acceso de red a un conjunto de recursos compartidos, escalables y elásticos, físicos o virtuales con aprovisionamiento de autoservicio y administración bajo demanda.

Una forma (un poco) más simple de describir la nube es que toma un conjunto de recursos, como procesadores y memoria, y los coloca en un grupo grande de recursos (en este caso, usando virtualización).

MODELO DE DEFINICIÓN



ISACA

CARACTERÍSTICAS ESENCIALES DE LA NUBE

Estas son las características que hacen que una nube sea una nube. Si algo tiene estas características, considérelo computación en la nube. Si carece de alguno de ellos, probablemente no sea una nube.

- La ***agrupación de recursos*** es la característica más fundamental, como se discutió anteriormente. El proveedor abstrae los recursos y los recopila en un grupo, partes de los cuales se pueden asignar a diferentes usuarios (generalmente basados en políticas).

- Los usuarios aprovisionan los recursos del grupo mediante el ***autoservicio*** bajo demanda. Ellos manejan sus propios recursos, sin tener que hablar con un administrador humano.

- El ***amplio*** acceso a la red significa que todos los recursos están disponibles en una red, sin necesidad del acceso físico directo; la red no es necesariamente parte del servicio.

CARACTERÍSTICAS ESENCIALES DE LA NUBE

- ***La elasticidad rápida*** permite a los usuarios ampliar o contraer los recursos que utilizan del grupo (aprovisionamiento y desaprovisionamiento), a menudo de forma completamente automática. Esto les permite relacionar más estrechamente el consumo de recursos con la demanda (por ejemplo, agregar servidores virtuales cuando la demanda aumenta y luego apagarlos cuando baja la demanda).

- ***Medidores de servicio*** que son proporcionados, para garantizar que los usuarios solo usen lo que se les ha asignado, y, si es necesario, cobrar por ello. Aquí es donde viene el término computación como servicio público (utility computing), ya que los recursos informáticos ahora se pueden consumir como el agua y la electricidad, el cliente solo paga por lo que usa.

ISACA Quito Chapter

Modelos de servicio

MODELOS DE SERVICIO

EI NIST define tres modelos de servicio que describen las diferentes categorías fundamentales de servicios en la nube:

- ***Software como servicio (SaaS)*** es una aplicación completa administrada y alojada por el proveedor. Los usuarios acceden a ella con un navegador web, una aplicación móvil o una aplicación de cliente liviana.

- ***Plataforma como Servicio (PaaS)*** abstrae y proporciona plataformas de desarrollo de aplicaciones, como bases de datos, plataformas de aplicaciones (por ejemplo, un lugar para ejecutar Python, PHP u otro código), almacenamiento de archivos y colaboración, o incluso procesamiento de aplicaciones propietarias (como aprendizaje de máquina, procesamiento de Big Data o acceso directo a interfaces de programación de aplicaciones (API) a características de una aplicación SaaS completa). EI diferenciador clave es que, con PaaS, no se maneja los servidores, redes u otra infraestructura subyacente.

- ***Infraestructura como servicio (IaaS)*** ofrece acceso a un conjunto de recursos de infraestructura base de informática, como computación, red o almacenamiento.

ISACA
Quito Chapter

Modelos de implementación

MODELOS DE IMPLEMENTACIÓN

- ***Nube pública:*** La infraestructura de la nube está disponible para el público en general o un gran grupo de la industria y es propiedad de una organización que vende servicios en la nube.

- ***Nube privada:*** La infraestructura de la nube se opera únicamente para una sola organización. Puede ser administrado por la organización o por un tercero y puede estar ubicado en sus instalaciones o fuera de su propiedad.

- ***Nube comunitaria:*** La infraestructura en la nube es compartida por varias organizaciones y soporta a una comunidad específica que tiene inquietudes compartidas (por ejemplo, misión, requisitos de seguridad, política o consideraciones de cumplimiento). Puede ser administrado por las organizaciones o por un tercero y puede estar ubicado en sus instalaciones o fuera de ellas.

- ***Nube híbrida:*** La infraestructura de la nube es una composición de dos o más nubes (privada, comunitaria o pública) que siguen siendo entidades únicas, pero están unidas por estándares o tecnología patentada que permite la portabilidad de datos y aplicaciones (por ejemplo, proliferación de nubes para equilibrar la carga entre nubes). El término Híbrido también se usa comúnmente para describir un centro de datos que no está en la nube y está conectado directamente a un proveedor de servicios en la nube.

MODELOS DE DESPLIEGUE DE LA NUBE

La nube se implementa con mayor frecuencia en uno de los tres modelos, a los que también se hace referencia con frecuencia como estructuras de nubes:

1. **Nube Pública**
- Infraestructura disponible para el público general (por ejemplo, Google Apps, Amazon EC2, Apple® iCloud).
- **Ubicación**: Se despliega fuera de la infraestructura empresarial, en la infraestructura del CSP (Proveedor de Servicios en la Nube).

2. **Nube Comunitaria**
- Infraestructura provisionada para el uso exclusivo de una comunidad específica de consumidores con preocupaciones compartidas (por ejemplo, industrias verticales, escuelas, investigadores, desarrolladores de software).
- **Ubicación**: Puede estar desplegada tanto in situ (dentro de la infraestructura empresarial) como fuera de ella (en la infraestructura del CSP, también llamado "subcontratado").

MODELOS DE DESPLIEGUE DE LA NUBE

3. Nube Privada

- Infraestructura

- utilizada exclusivamente por una única empresa.
- **Ubicación**: Similar a las nubes comunitarias, puede estar desplegada tanto in situ como fuera de las instalaciones empresariales.

4. Nube Híbrida

- Infraestructura compuesta por dos o más infraestructuras de nube distintas (privada, comunitaria o pública) que permanecen como entidades únicas

MODELOS DE IMPLEMENTACIÓN

	Infraestructura Propiedad de[1]	Infraestructura Propiedad de[2]	Infraestructura Localizada en[3]	Accesible y Consumidad por[4]
Pública	Proveedor externo	Proveedor externo	Instalación propia	No confiable
Privada/ Comunitaria	Organización / Proveedor Ext.	Organización / Proveedor Ext.	Instalación propia / Instalación Externa	Confiable
Híbrida	Organización y proveedor ext.	Organización y proveedor ext.	Instalación propia y externa	Confiable y no confiable

1. La administración incluye: gobierno, operaciones, seguridad, cumplimiento, etc.
2. La infraestructura implica infraestructura física, como instalaciones, redes informáticas y equipos de almacenamiento.
3. La ubicación de la infraestructura es tanto física como relativa al alcance de gestión de una organización y habla de propiedad versus control.
4. Los usuarios de confianza del servicio son aquellos que se consideran parte del alcance legal / contractual / político de una organización, incluidos empleados, contratistas y socios comerciales. Los usuarios que no son de confianza son aquellos que pueden estar autorizados para consumir algunos / todos los servicios, pero no son extensiones lógicas de la organización.

Tenancy

En computación en la nube, un "tenant" (o "inquilino" en español) se refiere a una instancia individual o entidad que utiliza los recursos compartidos de una plataforma de computación en la nube. Aquí hay una explicación más detallada:

Multitenancy

La computación en la nube a menudo utiliza un modelo de "multitenancy" (multialojamiento), en el cual múltiples tenants comparten los mismos recursos físicos o lógicos de la infraestructura de la nube. Cada tenant se aísla virtualmente de los demás, aunque comparten los mismos recursos subyacentes. Este modelo es eficiente en términos de costos y recursos, ya que permite a los proveedores de servicios en la nube (CSP) servir a muchos clientes desde una sola infraestructura.

Tipos de Tenancy

1. Single-tenant (alojamiento único)

- Definición: Un solo tenant tiene dedicados todos los recursos de la infraestructura.
- Ventajas: Mayor control, personalización y seguridad, ya que no se comparte con otros tenants.
- Desventajas: Generalmente, es más costoso y menos eficiente en el uso de recursos.

2. Multi-tenant (multialojamiento):

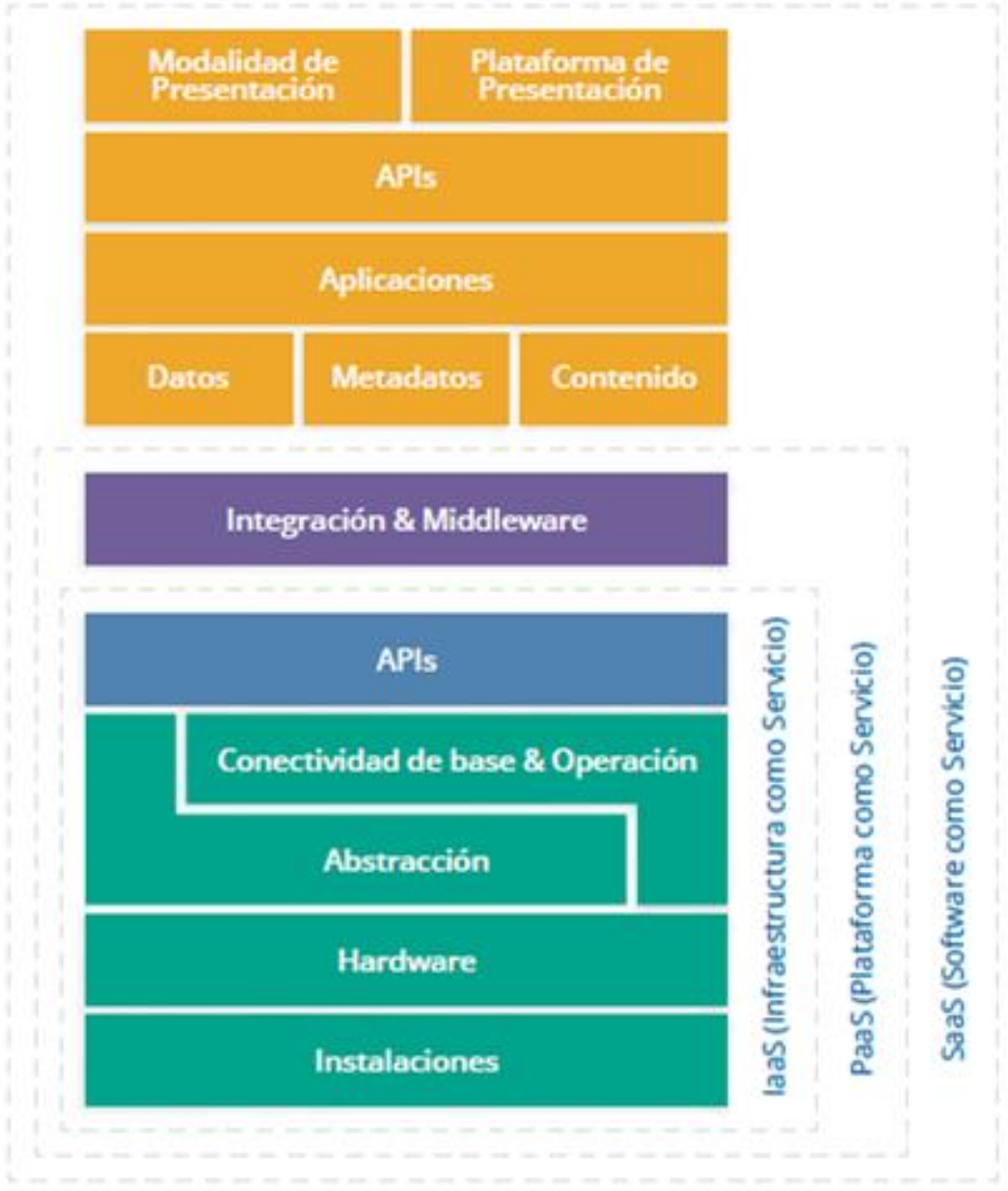
- Definición: Varios tenants comparten los mismos recursos de infraestructura, pero con un aislamiento lógico.
- Ventajas: Costos reducidos y mayor eficiencia en el uso de recursos.
- Desventajas: Menos personalización y potencialmente mayores preocupaciones de seguridad, aunque los CSP suelen implementar medidas estrictas para garantizar el aislamiento y la seguridad de los datos.

ISACA
Quito Chapter

Modelos de referencia y arquitectura

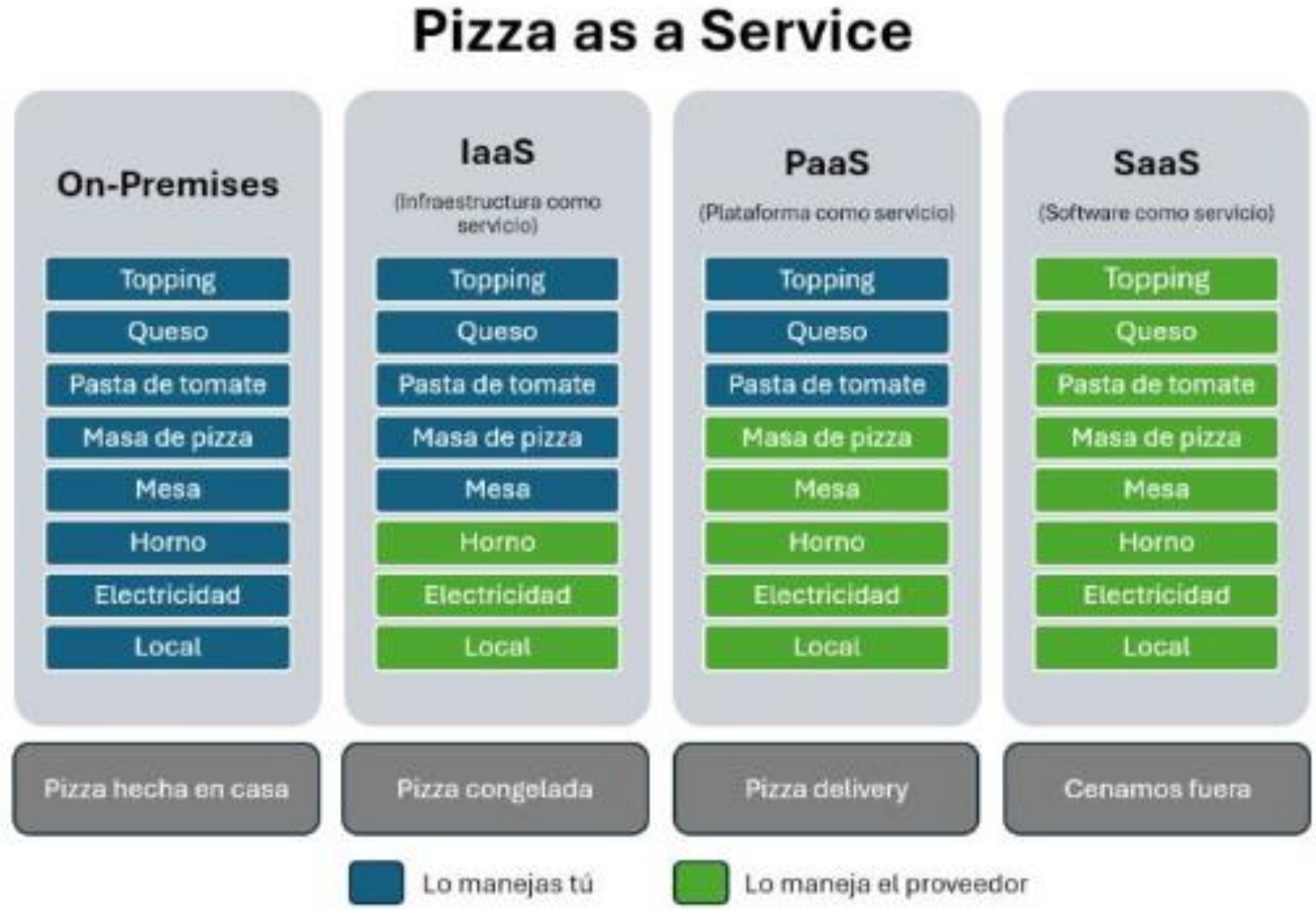
MODELOS DE REFERENCIA Y ARQUITECTURA

Una forma de ver la computación en la nube es como una pila donde el Software como Servicio se basa en la Plataforma como Servicio, que a su vez se basa en la Infraestructura como Servicio. Esto no es representativo de todas (o incluso la mayoría) de las implementaciones del mundo real, pero sirve como una referencia útil para iniciar la discusión.

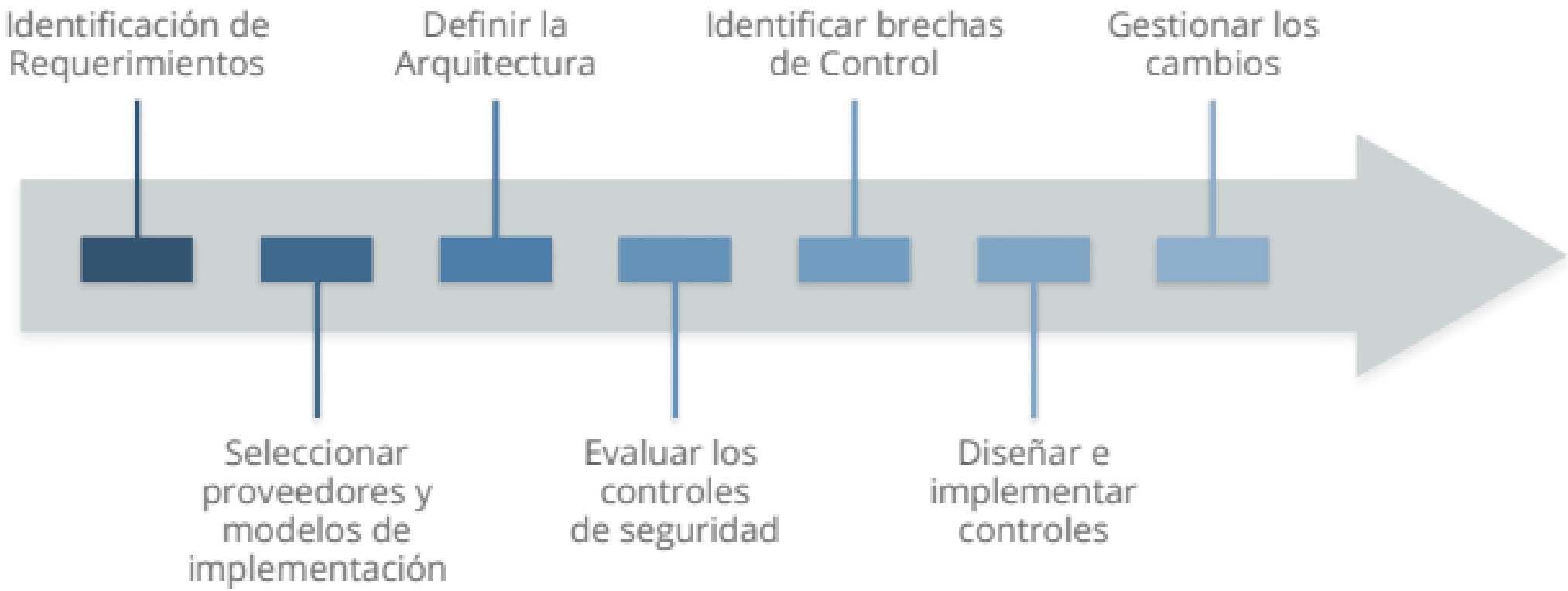


ALCANCE Y RESPONSABILIDADES DE LA SEGURIDAD EN LA NUBE Y EL CUMPLIMIENTO

ALCANCE Y RESPONSABILIDADES DE LA SEGURIDAD EN LA NUBE Y EL CUMPLIMIENTO



MODELO SIMPLE DE PROCESO DE SEGURIDAD EN LA NUBE



EL ELEMENTO CLAVE DE LA CONFIANZA

- ***Desafíos:*** La seguridad y la privacidad de los datos se ven comúnmente como barreras críticas para la adopción de servicios en la nube.

- ***Mitigación de Riesgos:*** Los usuarios pueden optar por establecer acuerdos de nivel de servicio (SLAs) o solicitar a los proveedores de servicios en la nube que cumplan con objetivos de control específicos.

- ***Confianza:*** Es un componente mayor en el modelo de negocio de la computación en la nube. La relación cliente-proveedor debe fundamentarse en la confianza para superar todas las preocupaciones.

- ***Consideraciones para la Adopción:*** Es crucial conocer a todas las partes involucradas y sus ubicaciones físicas, incluyendo al CSP, sus empleados y cualquier vendedor en contacto cercano que pueda acceder a los datos del usuario. Se recomienda elegir CSPs con un historial significativo en la industria de servicios en la nube y que puedan proporcionar referencias comerciales sólidas.

EL ELEMENTO CLAVE DE LA CONFIANZA

Aspectos Influenciadores en la Confianza sobre un CSP:

- Posibilidad de auditoría y verificación de controles.
- Posición financiera del CSP y reconocimiento en el mercado.
- Certificaciones o reconocimientos de estándares de seguridad por autoridades.
- Disponibilidad de planes de continuidad empresarial, planes de recuperación de desastres y procedimientos robustos de respaldo.
- Calidad de los propios datos del usuario y clasificación de datos; políticas, principios y marcos; procesos; estructuras organizativas; cultura, ética y comportamiento; infraestructura y aplicaciones de servicios; habilidades y competencias del personal; y apetito por el riesgo.
- Negociaciones generales y relación con el proveedor de servicios: contratos, SLAs, procesos de comunicación, matrices de roles y responsabilidades, etc.

ACTIVOS DE INFORMACIÓN Y RIESGO

Los activos de información pueden ser aproximadamente categorizados como datos, aplicaciones y procesos. Estos activos comúnmente están sujetos a los siguientes eventos de riesgo:

- ***Indisponibilidad***: El activo no está disponible y no puede ser usado o accedido por la empresa. La causa puede ser accidental (falla de la infraestructura), intencional (ataques de denegación de servicio distribuido [DDoS]) o legal (citación de la base de datos que contiene todos los datos en un caso de arquitectura de multitenencia donde los datos de un cliente están sujetos a investigación legal).

- ***Pérdida:*** El activo se pierde o destruye. La causa puede ser accidental (desastre natural, manipulación incorrecta, etc.) o intencional (destrucción deliberada de datos).

- ***Robo***: El activo ha sido robado intencionalmente y ahora está en posesión de otro individuo/empresa. El robo es una acción deliberada que puede implicar pérdida de datos.

- ***Divulgación:*** El activo ha sido liberado a personal/empresas/organizaciones no autorizadas o al público. La divulgación puede ser accidental o deliberada. Esto también incluye el acceso no deseado, pero legal, a datos debido a diferentes regulaciones entre fronteras internacionales.

ACTIVOS DE INFORMACIÓN Y RIESGO

Los datos son comúnmente los activos más valiosos y los objetivos más probables de ataques en la nube. Sin embargo, es importante no pasar por alto el riesgo relacionado con aplicaciones y procesos. El impacto comercial de largos ataques DDoS no siempre puede ser absorbido por una empresa; aunque no se sufra pérdida o divulgación de datos.

Figure 2—Impact of Risk Events on Assets

Type	Unavailability	Loss	Theft	Disclosure
Data	Disruption of activities; lack of resources to keep on with "business as usual;" possibility of data poisoning	Disruption of activities; required activation of backup restore procedures (DRP); possibility of partial loss of the asset (depending on the recovery point objective [RPO]); financial loss associated with recovery efforts	Business competitive disadvantage; possibility of blackmail; loss of credibility with customers/clients	Damage to company reputation or image; possibility of regulatory sanctions; financial impact
Applications/ processes	Disruption of activities; lack of resources to keep on with "business as usual"		Higher risk/threat of more selective attacks to data	

CONSIDERACIONES DE SEGURIDAD EN IaaS

Con la infraestructura como servicio (IaaS), el proveedor de servicios en la nube (CSP) proporciona a la empresa recursos/equipos informáticos fundamentales (almacenamiento, hardware, servidores y componentes de red) mientras que la empresa sigue teniendo el control del sistema operativo (SO) y las aplicaciones instaladas.

Factores que Disminuyen el Riesgo:

- Escalabilidad, elasticidad, procedimientos de recuperación de desastres y de respaldo, y la gestión de parches, que contribuyen a reducir los riesgos de indisponibilidad, pérdida, robo y divulgación.

Factores que Aumentan el Riesgo:

- Incluye requisitos legales transfronterizos, fallos de aislamiento y multitenencia, falta de visibilidad sobre las medidas de seguridad técnica, ausencia de planes de recuperación ante desastres (DRP) y procedimientos de respaldo, preocupaciones sobre la seguridad física, problemas de disposición de datos, infraestructura offshore, mantenimiento de la seguridad de máquinas virtuales, y autenticidad del proveedor de la nube.

CONSIDERACIONES DE SEGURIDAD EN PaaS

PaaS agrega funcionalidad a IaaS permitiendo desplegar aplicaciones en la infraestructura en la nube, con el CSP encargándose del soporte físico, sistema operativo y herramientas de programación. La empresa mantiene el control de las aplicaciones y los datos.

Factores que Disminuyen el Riesgo:

- Tiempos de desarrollo más cortos, impactando positivamente la indisponibilidad y pérdida.

Factores que Aumentan el Riesgo:

- Problemas de mapeo de aplicaciones, vulnerabilidades relacionadas con SOA y preocupaciones sobre la disposición de aplicaciones. Estos pueden introducir vulnerabilidades adicionales y afectar la seguridad relacionada con el robo, la divulgación, la indisponibilidad y la pérdida.

CONSIDERACIONES DE SEGURIDAD EN SaaS

En el modelo SaaS, el proveedor de servicios en la nube proporciona aplicaciones que se ejecutan en la infraestructura en la nube, mientras que la empresa proporciona los datos necesarios. La responsabilidad de la infraestructura física, el sistema operativo, las aplicaciones y los datos recae en el proveedor de servicios. La empresa actúa solo como cliente o usuario.

Factores que Disminuyen el Riesgo:

- Medidas de seguridad mejoradas y la gestión de parches de aplicaciones, que suelen gestionarse de manera más efectiva debido a la naturaleza centralizada de las ofertas de SaaS.

Factores que Aumentan el Riesgo:

- Preocupaciones sobre la propiedad de los datos, disposición de datos, falta de visibilidad en el ciclo de vida de desarrollo de sistemas de software (SDLC), desafíos de gestión de identidad y acceso (IAM), complejidades de la estrategia de salida, amplia exposición de aplicaciones, la facilidad de contratar soluciones SaaS eludiendo el cumplimiento, falta de control sobre el proceso de gestión de lanzamientos, y vulnerabilidades del navegador. Estos factores pueden llevar a riesgos en indisponibilidad, pérdida, robo y divulgación.

FACTORES DE RIESGO POR MODELO DE IMPLEMENTACIÓN

Los modelos de despliegue en la nube no tienen la misma abstracción que los modelos de servicio en la nube. Es decir, el riesgo no es acumulativo, sino particular a cada modelo.

La "confianza" entre las diferentes entidades (proveedores de servicios en la nube, clientes, proveedores de servicios de terceros de CSP, etc.) es un factor importante, no solo la confianza entre el CSP y el cliente, sino también suficiente confianza en los otros inquilinos que comparten recursos informáticos alojando los activos de información de la empresa.

Si un usuario abusa de la infraestructura y servicios de la nube pública, toda la infraestructura podría estar en riesgo de falla, robo o incautación (para forenses), incluyendo los servicios utilizados por otras empresas. Es importante como parte del proceso de decisión considerar cuidadosamente qué activos pueden ser alojados de manera segura en una nube pública y cuáles no.

FACTORES DE RIESGO POR MODELO DE IMPLEMENTACIÓN

D1. Nube Pública (Public Cloud)

- En una nube pública, el proveedor de servicios en la nube (CSP) comparte infraestructura y recursos entre varias empresas e individuos no relacionados.

Factores que Disminuyen el Riesgo:

- *D1.A Reputación Pública:* Los proveedores son conscientes de la percepción de mayor riesgo y trabajan activamente para mantener una buena reputación de seguridad.

Factores que Aumentan el Riesgo:

- *D1.B Compartición Total de la Nube (Agrupación de Datos):* La infraestructura es compartida por múltiples inquilinos sin relación, lo que aumenta los riesgos de seguridad.

- *D1.C Daños Colaterales:* Un ataque a un inquilino puede afectar a otros debido a la compartición de recursos.

FACTORES DE RIESGO POR MODELO DE IMPLEMENTACIÓN

D2. Nube Comunitaria (Community Cloud)

- Servicios de nube desplegados para el uso de un grupo de entidades que comparten un nivel inherente de "confianza".

Factores que Disminuyen el Riesgo:

- *D2.A Grupo de Entidades Similar:* La existencia de confianza entre las entidades reduce los riesgos comparados con la nube pública.

- *D2.B Acceso Dedicado para la Comunidad:* Se puede configurar acceso dedicado solo para usuarios autorizados de la comunidad.

Factores que Aumentan el Riesgo:

- *D2.C Compartición de la Nube:* Diferentes entidades pueden tener medidas de seguridad o requisitos divergentes, lo que podría aumentar el riesgo.

FACTORES DE RIESGO POR MODELO DE IMPLEMENTACIÓN

D3. Nube Privada (Private Cloud)

- Servicios de nube desplegados para el uso exclusivo de una empresa. No se permite la interacción con otras entidades dentro de la nube.

Factores que Disminuyen el Riesgo:

- *D3.A Construcción en las Instalaciones:* Permite un control más estrecho de consideraciones físicas o de ubicación.

- *D3.B Rendimiento:* Para nubes privadas locales, las tasas de transferencia son más altas y la capacidad de almacenamiento puede ser superior.

Factores que Aumentan el Riesgo:

- *D3.C Compatibilidad de Aplicaciones:* Problemas con software antiguo o personalizado que asume acceso directo a los recursos.

- *D3.D Inversiones Requeridas:* La necesidad de justificar los gastos frente a la percepción de que la nube elimina la necesidad de infraestructura física.

FACTORES DE RIESGO POR MODELO DE IMPLEMENTACIÓN

D4. Nube Híbrida (Hybrid Cloud)

- Modelo que permite a las empresas crear una mezcla de nubes públicas, comunitarias y privadas dependiendo del nivel de "confianza" requerido para sus activos de información.

Factores que Aumentan el Riesgo:

- *D4.A Interdependencia de la Nube:* La mezcla de diferentes tipos de nubes requiere controles de identidad estrictos y credenciales fuertes para permitir el acceso entre ellas.

PROCESO DE MODELADO DE AMENAZAS EN LA NUBE

La modelización de amenazas es crucial para anticipar y mitigar ataques cibernéticos, especialmente en el dinámico entorno de la nube.

Responsables de la Modelización de Amenazas en la Nube

- La modelización de amenazas en la nube requiere de un equipo con conocimientos tanto en seguridad como en tecnologías de nube.

- Roles como arquitectos de aplicación, arquitectos de nube y analistas de seguridad son fundamentales para liderar el proceso de modelización de amenazas.

Aunque el proceso es similar al de la modelización de amenazas no basadas en la nube, se enfatiza en:

- La revisión holística de la infraestructura de nube y la comprensión del Modelo de Servicio de Nube (IaaS, PaaS, SaaS) y el modelo de responsabilidad compartida.

- Identificar objetivos de seguridad específicos para la nube, establecer el alcance de la evaluación, descomponer el sistema y sus aplicaciones, identificar y calificar amenazas, identificar debilidades y diseñar y priorizar mitigaciones.

PROCESO DE MODELADO DE AMENAZAS EN LA NUBE

Actividades Centrales de la Modelización de Amenazas

1. **Identificar Objetivos de Seguridad**: Determinar los objetivos de seguridad de la organización y la arquitectura del sistema.

1. **Definir el Alcance de la Evaluación:** Comprender el sistema o aplicaciones bajo revisión.

1. **Descomposición del Sistema y Aplicaciones:** Analizar componentes y sus interacciones.

1. **Identificar y Calificar Amenazas:** Utilizar recursos de la industria como CSA Top Threats para identificar amenazas únicas en la nube.

1. **Identificar Debilidades y Diseñar Mitigaciones:** Considerar debilidades comunes en el diseño e implementación en la nube y enfocarse en controles de seguridad específicos.

1. **Comunicación y Acción:** Hacer que los datos del modelado y las decisiones de diseño de seguridad sean conocidos.

1. **Reevaluación Periódica:** Mantener el modelo de amenazas actualizado con los cambios en la arquitectura y las nuevas amenazas.

REFERENCIA DEL MODELO DE AMENAZAS EN LA NUBE

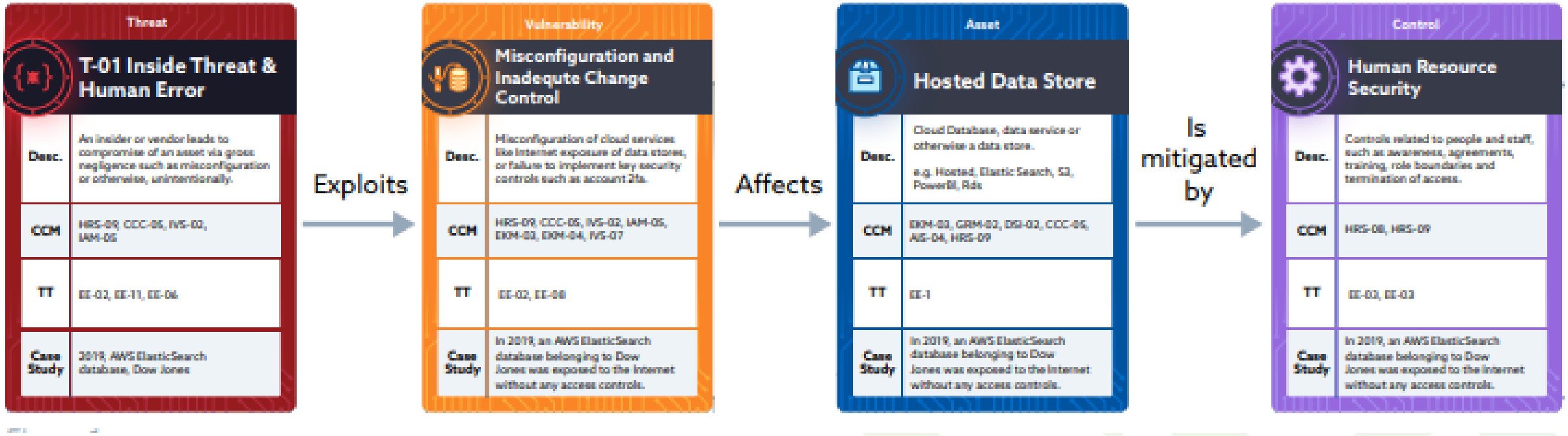
Ejemplo práctico de cómo se puede aplicar la modelización de amenazas en la nube utilizando el caso de exposición de datos de Dow Jones en 2019 como referencia:

- **Actor**: Un proveedor autorizado de terceros para Dow Jones no protegió con contraseña una base de datos Elasticsearch alojada en AWS perteneciente a Dow Jones, lo que resultó en una vulnerabilidad significativa.

- **Ataque**: La base de datos, al no tener protección por contraseña, estaba accesible para cualquiera sin restricciones y podía ser encontrada mediante motores de búsqueda de IoT comúnmente disponibles. La base de datos mal configurada fue descubierta en 2019 por un investigador de seguridad, quien informó a Dow Jones sobre el problema.

- **Vulnerabilidades**: La principal vulnerabilidad fue que la base de datos de Dow Jones no estaba protegida con contraseña por uno de sus proveedores de seguridad autorizados y presumiblemente confiables.

REFERENCIA DEL MODELO DE AMENAZAS EN LA NUBE



REFERENCIA DEL MODELO DE AMENAZAS EN LA NUBE

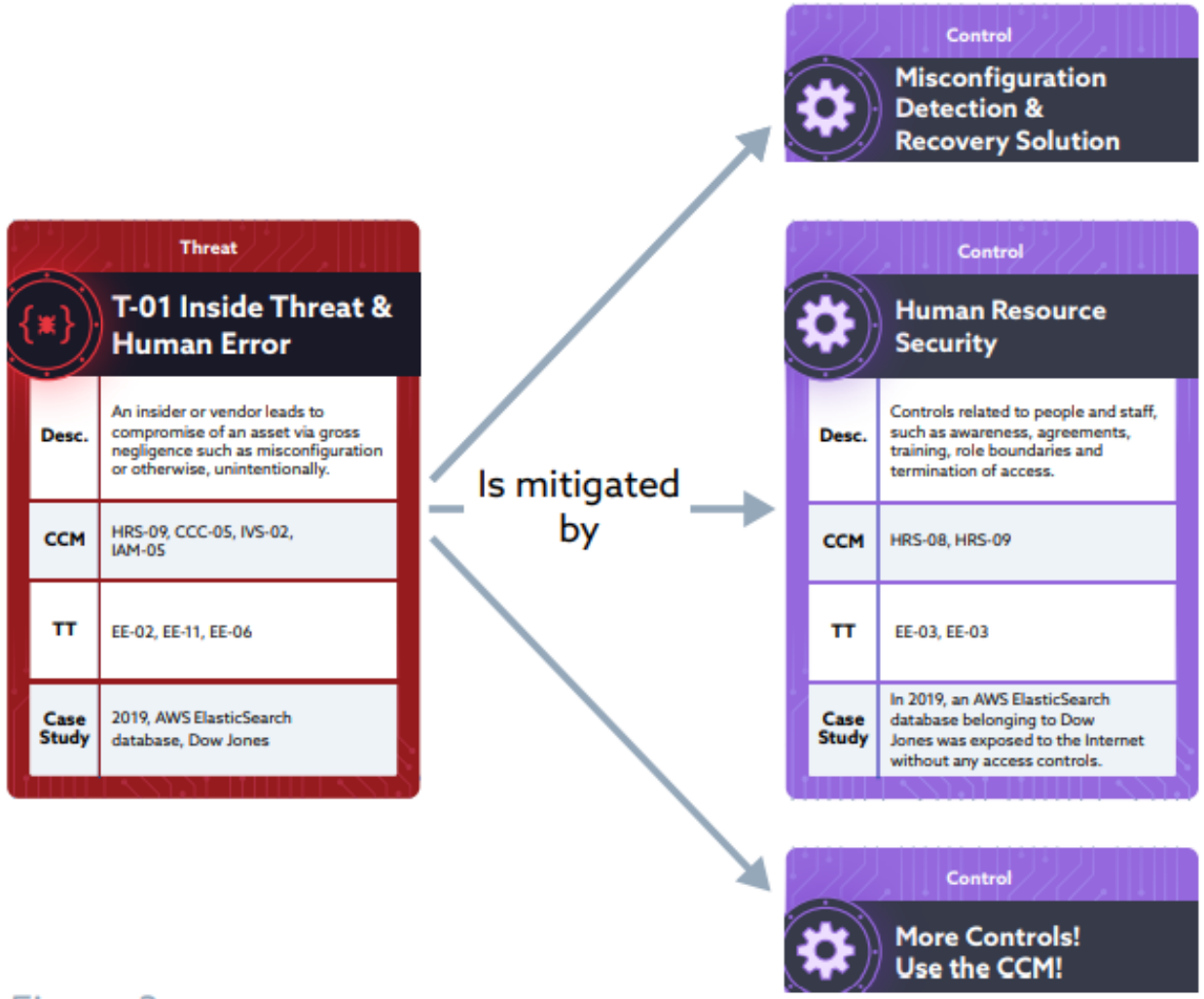


Figure 2

GOBERNANDO LA NUBE

Dominio	Título	Descripción
2	Gobernanza y gestión de riesgos empresariales	La capacidad de una organización para gobernar y medir el riesgo empresarial introducido por la computación en la nube. Elementos como la precedencia legal para infracciones de acuerdos, capacidad de las organizaciones de usuarios para evaluar adecuadamente el riesgo de un proveedor de servicios en la nube, responsabilidad de proteger datos confidenciales cuando tanto el usuario como el proveedor pueden tener la culpa, y cómo las fronteras internacionales pueden afectar estos problemas.
3	Asuntos legales: Contratos y descubrimiento electrónico	Posibles problemas legales al usar la computación en la nube. Las cuestiones que se abordan en esta sección incluyen los requisitos de protección para la información y los sistemas informáticos, las leyes de divulgación de violaciones de seguridad, los requisitos reglamentarios, los requisitos de privacidad, las leyes internacionales, etc.
4	Gestión de cumplimiento y auditoría	Mantener y probar el cumplimiento cuando se utiliza la computación en la nube. Aquí se tratan cuestiones relacionadas con la evaluación de cómo la computación en la nube afecta al cumplimiento de las políticas de seguridad interna, así como los diversos requisitos de cumplimiento (normativo, legislativo y de otro tipo). Este dominio incluye alguna dirección para probar el cumplimiento durante una auditoría.
5	Gobierno de la información	Gobernando los datos que se colocan en la nube. Aquí se discuten los elementos que rodean la identificación y el control de los datos en la nube, así como los controles de compensación que se pueden usar para lidiar con la pérdida de control físico cuando se mueven datos a la nube. Se mencionan otros elementos, como quién es responsable de la confidencialidad de los datos, la integridad y la disponibilidad.

OPERANDO EN LA NUBE

Dominio	Título	Descripción
6	Plan de Gestión y Continuidad del Negocio	Asegurar el plan de gestión y las interfaces administrativas utilizadas al acceder a la nube, incluidas las consolas web y las *API*. Garantizar la continuidad del negocio para implementaciones en la nube.
7	Seguridad de Infraestructura	Seguridad del núcleo de la infraestructura de la nube, incluidas las redes, la seguridad de la carga de trabajo y las consideraciones de la nube híbrida. Este dominio también incluye fundamentos de seguridad para nubes privadas.
8	Virtualización y contenedores	Seguridad para hipervisores, contenedores y redes definidas por software.
9	Respuesta a incidentes, notificación y remediación	Detección, respuesta, notificación y reparación adecuada de incidentes. Esto intenta abordar los elementos que deberían estar en su lugar, tanto a nivel de proveedor como de usuario, para permitir el manejo adecuado de incidentes y análisis forense. Este dominio lo ayudará a comprender las complejidades que trae la nube a su programa actual de manejo de incidentes.
10	Seguridad de aplicaciones	Asegurar el software de la aplicación que se ejecuta o se está desarrollando en la nube. Esto incluye elementos tales como si es apropiado migrar o diseñar una aplicación para que se ejecute en la nube y, de ser así, qué tipo de plataforma en la nube es la más adecuada (*SaaS*, *PaaS* o *IaaS*).
11	Seguridad y cifrado de datos	Implementando la seguridad y el cifrado de datos, y garantizando la administración escalable de claves.

OPERANDO EN LA NUBE

12	Identidad, derecho y administración de acceso.	Administrar identidades y aprovechar los servicios de directorio para proporcionar control de acceso. La atención se centra en los problemas que se encuentran al extender la identidad de una organización a la nube. Esta sección proporciona información sobre cómo evaluar la preparación de una organización para llevar a cabo una Gestión de acceso, idoneidad e identidad (*IdEA*) basada en la nube.
13	Seguridad como servicio	Proporcionar aseguramiento de seguridad facilitado por terceros, administración de incidentes, certificación de cumplimiento y supervisión de identidad y acceso.
14	Tecnologías relacionadas	Tecnologías establecidas y emergentes con una estrecha relación con la computación en la nube., incluidas el *Big Data*, el Internet de las cosas y la informática móvil.

ESTRUCTURA DEL CCM

El CCM v4.0 está estructurado en 17 dominios de seguridad y 197 controles. Los 17 dominios se basaron en el documento de orientación de seguridad de CSA e inspirados en marcos principales, como ISO/IEC 27007 e ISO/IEC 27002. Cada dominio de CCM define en qué categoría cae un control. El CCM fue diseñado deliberadamente como marcos de seguridad de la información líderes no relacionados con la nube para aprovechar la familiaridad con esos marcos existentes.

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

DESCRIPCIÓN DE LOS DOMINIOS CCM

Cada dominio se centra en una área específica de la seguridad en la nube, ofreciendo un conjunto de controles diseñados para mitigar riesgos y asegurar las operaciones en entornos de nube. Aquí se detallan los propósitos y los aspectos clave de cada dominio:

Audit and Assurance (A&A): Se centra en definir e implementar un proceso de gestión de auditoría, con seis especificaciones de control, para soportar la planificación de auditorías, análisis de riesgos, evaluación de controles de seguridad, y generación de informes de remediación.

Application and Interface Security (AIS): Incluye siete controles para guiar a las organizaciones hacia el diseño seguro, desarrollo, despliegue y operaciones de aplicaciones e interfaces en la nube, alineando los objetivos de seguridad de AIS con los objetivos empresariales y el cumplimiento regulatorio.

DESCRIPCIÓN DE LOS DOMINIOS CCM

Business Continuity Management and Operational Resilience (BCR):

- Orientado a garantizar la dependabilidad de los servicios en la nube con once especificaciones de control que guían estrategias de resiliencia, incluyendo el desarrollo de planes de mitigación y continuidad del negocio ante interrupciones.

Change Control and Configuration Management (CCC):

- Integra nueve controles para mitigar los riesgos asociados con los cambios de configuración en los activos de TI, asegurando que las modificaciones se realicen según una línea base aprobada

DESCRIPCIÓN DE LOS DOMINIOS CCM

Cryptography Encryption and Key Management (CEK):

Con veintiún especificaciones de control, este dominio asegura que los datos y las claves se utilizan para proteger y asegurar adecuadamente los datos, abarcando la gestión de riesgos, políticas y procedimientos de criptografía.

Datacenter Security (DCS):

Proporciona quince controles para las organizaciones que ofrecen servicios de hospedaje en centros de datos, protegiendo los datos de los clientes en el centro de datos.

Data Security & Privacy (DSP):

Un nuevo dominio en CCM v4.0 con diecinueve controles sobre privacidad y seguridad de los datos, no específico de la industria, centrado en las necesidades de protección de datos globales.

DESCRIPCIÓN DE LOS DOMINIOS CCM

Interoperability and Portability (IPY):

- Con cuatro controles, este dominio aborda la interoperabilidad y la portabilidad en la nube, enfocándose en la capacidad de trabajar juntos de los componentes del sistema y en mover componentes de una nube a otra

Infrastructure and Virtualization Security (IVS):

- Guía la implementación de controles para asegurar infraestructuras y tecnologías de virtualización con nueve especificaciones de control.

Logging and Monitoring (LOG) :

- Enfatiza la importancia del registro y monitoreo para la seguridad de las operaciones en la nube, con trece controles centrados en la gobernanza y los procesos.

Security Incident Management, E-Discovery, and Cloud Forensics (SEF):

- Ocho controles diseñados para asegurar que las políticas y procedimientos establecidos respondan adecuadamente a incidentes de seguridad.

DESCRIPCIÓN DE LOS DOMINIOS CCM

Supply Chain Management, Transparency, and Accountability (STA):

- Describe un conjunto de controles para la gestión de riesgos de la cadena de suministro, incluyendo la transparencia y la rendición de cuentas con catorce especificaciones de control.

Threat and Vulnerability Management (TVM):

- Este dominio incluye diez controles enfocados en identificar y mitigar vulnerabilidades que afectan la infraestructura de una organización. Se ocupa de la gestión de riesgos, la prevención de malware, la detección de vulnerabilidades, y la realización de pruebas de penetración para proteger contra amenazas a la seguridad.

Universal Endpoint Management (UEM):

- Dirigido a gestionar los riesgos de los dispositivos finales, especialmente en entornos móviles y remotos. Este dominio abarca catorce controles que incluyen la administración de inventario de dispositivos, la implementación de políticas de seguridad, el cifrado de datos y la prevención de pérdida de datos para asegurar el uso seguro de dispositivos dentro y fuera de la oficina.

ISACA Quito Chapter

MUCHAS GRACIAS

+593 995061566
https://www.linkedin.com/in/jclopezexacta/