Seguridad en la Nube Pública: *Landing Zone*

Javier Martínez,

Developer Advocate en Google Cloud Platform

Javier Martínez

Javier es responsable del equipo de preventa en Google Cloud desde el año 2017. Apasionado por la tecnología, cuenta con una amplia experiencia en infraestructuras de TI en la nube, networking, servidores Unix y Linux, y almacenamiento. Javier es un profesional con múltiples certificaciones técnicas y un amplio conocimiento del mercado TI profesional, así como de las tendencias tecnológicas en general. Antes de unirse al equipo de Google Cloud, trabajó 12 años en NetApp, compañía de soluciones de gestión de datos.

Índice

01 Beneficios de la nube pública y la importancia de un modelo adecuado de seguridad

En los últimos años hemos observado un incremento en la adopción de las tecnologías cloud por parte de organizaciones de todo tipo y tamaño que buscan aumentar la productividad y la colaboración *online* para ser más eficientes y competitivas. Sin embargo, ante los confinamientos y restricciones a la movilidad derivados de la pandemia, esta adopción se está acelerando como una expresión de la resiliencia necesaria para que las compañías salgan adelante.

Hay algunas cifras que, precisamente, explican el panorama actual y futuro: **en la actualidad el 75% de las empresas que utilizan la nube ya emplean una estrategia *cloud-first*,** en la que marcan la pauta a seguir en sus estrategias de negocio. Igualmente, para el año 2025 la mitad de las cargas de trabajo de las grandes organizaciones se encontrará en la nube.

Esta tendencia en la adopción de una estrategia *cloud-first*[1] se explica también gracias a los múltiples beneficios que aporta este paradigma a las compañías, como, por ejemplo:

[1] Una estrategia cloud-first es aquella en la que una organización prioriza la implementación y el uso de servicios y productos en la nube.

- **Reducción de los costes operativos** gracias a que es un tercero quien se encarga del mantenimiento de la infraestructura y las operaciones, evitando gastos de capital asociados. Esto permite una mayor inversión en otras partidas que aporten valor a la compañía. De hecho, de acuerdo con un estudio de Hosting Tribunal, la media de ahorro del gasto TI con la migración a la nube es de un 15%, siendo las PYMES las que registrarían una reducción mayor del gasto, de hasta un 36%. "Guía para el buen gobierno financiero en la nube"
- **Flexibilidad y escalabilidad** para ajustarse fácilmente a las necesidades de crecimiento de cada organización. Con este tipo de estrategias los decisores pueden hacer una mejor gestión de los recursos disponibles, dedicándolos a las necesidades de cada momento. Esta es una característica muy útil en sectores como el *media*, por ejemplo: en los picos de tráfico se pueden destinar más recursos, y volver a reducir la asignación tan pronto como se estabilice dicho tráfico o haya una caída del mismo.
- **Analítica de datos empresariales.** El valor que tienen los datos propios es incalculable; gracias a ellos y a su análisis, una empresa puede, por ejemplo, mejorar el ROI en sus estrategias de marketing gracias a un *retargeting* más focalizado, o extraer conclusiones objetivas sobre qué está funcionando bien y qué necesita mejorar en sus procesos. El mercado del big data y el analytics crecerá este año hasta alcanzar ingresos de 215.700 mil millones de dólares, de acuerdo con IDC, lo que pone de manifiesto la importancia de la analítica de datos.

75%
de empresas utilizan la **nube** ya emplean una estrategia ***cloud-first***

- **Mayor accesibilidad a nuevas tecnologías** para todo tipo de compañías. Si una empresa tiene puesto el foco en la nube, y sus recursos – tanto humanos como técnicos – están preparados para su uso y adopción, las posibilidades de acceso a nuevas tecnologías e innovaciones de forma ágil son mucho mayores. Esto les permitirá tener una posición ventajosa en su mercado, así como hacer frente rápida y eficazmente a posibles disrupciones del mismo o a cambios en la demanda. Encontramos innovaciones *cloud* avanzadas en múltiples sectores, desde el industrial al turístico. Por ejemplo, el grupo hotelero multinacional Meliá Hotels ha situado a las tecnologías cloud en el centro de su estrategia de negocio, con el objetivo primordial de incrementar el customer *engagement* a través de la colaboración entre todas las áreas de la organización, en todos los países.
- **Desarrollo ágil de productos** que permite acortar el tiempo de comercialización de soluciones. Esto se traduce en una mayor competitividad y, por ende, en un crecimiento en el reconocimiento de marca y en los beneficios finales.

Toda estrategia *cloud-first* debe implementarse bajo el paraguas de la **seguridad.** De lo contrario, la aproximación a la nube será incompleta y no podrá ofrecer ni la fiabilidad necesaria ni la protección de datos, aplicaciones y servicios críticos imprescindibles para las organizaciones. La premisa de la que parte un buen modelo de seguridad TI es que su infraestructura en la nube **no dependa de una sola tecnología o solución**, sino que se construya con varias capas, teniendo en cuenta factores como:

- **Una infraestructura** que implemente prácticas de seguridad TI rigurosas, con equipos operativos que detecten las amenazas contra las infraestructuras y respondan ante ellas 24/7.
- **Un cifrado de las comunicaciones** que proteja los datos mientras están en tránsito. Además, su infraestructura y su red deben tener varias capas de protección para defender a los clientes contra ataques de denegación del servicio.
- **Un acceso seguro** mediante la autenticación de los usuarios y los servicios. Hay que proteger el acceso a los datos sensibles con **herramientas avanzadas, como las llaves de seguridad Titan,** diseñadas a prueba de suplantación de identidad.

- **Una protección de los datos almacenados contra** el acceso no autorizado y las interrupciones de servicio.
- **Un enfoque *Zero Trust*,** que monitoriza y autentifica continuamente a los usuarios que acceden a la red de la organización.
- **Seguridad del hardware utilizado,** desde los servidores y los equipos de redes, hasta la pila de *software* de nivel bajo que se ejecuta en cada máquina.
- **Una defensa de los centros de datos y el acceso a sus instalaciones** a través de capas de seguridad que incluyan, por ejemplo, tarjetas de acceso electrónicas personalizadas, alarmas, barreras de acceso para vehículos, biometría, etc.
- **Disponibilidad continua de los servicios** para cumplir con los estándares de alto nivel en cuanto a rendimiento, resiliencia, disponibilidad, precisión y seguridad.

Por último, una infraestructura de nube segura también debe disponer de **redes troncales que conecten entre sí sus centros de datos y sean de su total propiedad.** Así, si el tráfico de una organización se encuentra en esta red, se minimiza el riesgo de que sea objeto de ciberataques.

Una vez comprobado que la nube pública elegida cuenta con los factores de seguridad antes mencionados, **es altamente recomendable que la planificación de la migración a la nube pública se haga en un entorno TI separado y con control absoluto.** De esta forma, apenas existen riesgos que puedan afectar a la continuidad del negocio o a los datos de la organización. Este entorno se conoce como ***landing zone.***

> **Una landing zone es un conjunto de procesos y herramientas que permiten a una organización comenzar a utilizar servicios en la nube de manera controlada.**

02
Comenzar de forma segura con una *landing zone*

Una landing zone es un conjunto de procesos y herramientas que permiten a una organización comenzar a utilizar servicios en la nube de manera controlada, ya que sirven como base sobre la que "aterrizar" y desplegar de forma segura y segregada las infraestructuras, servicios TI y cargas de trabajo en la nube.

Su principal objetivo es **desplegar de forma independiente un entorno TI** en la nube pública sobre el cual tener pleno control. Generar una landing zone bajo el paraguas de **una plataforma con un modelo de seguridad adecuado es lo más recomendable.** Además, es **altamente replicable**: mediante procesos automatizados, los equipos de TI pueden repetir después modelos de *landing zone* previamente generados en nuevos proyectos o para otras áreas o departamentos.

Para tener este control, una arquitectura típica de *landing zone* se sirve de una cuenta de gestión centralizada, pero también permite **generar otros subroles y cuentas dentro de la organización.** De esta forma, se pueden segregar las funciones financieras, administrativas y operativas con diferentes grados y niveles de roles y permisos de acceso, en función de sus necesidades específicas.

Otro aspecto importante es que facilita la creación de nuevas redes y extensiones a centros de datos. Con las *landing zones* **se pueden definir subredes y elegir los direccionamientos más adecuados para que la organización disponga de la conectividad y latencia más adecuadas.** Para ello, se pueden tener en cuenta múltiples criterios, los requisitos de las diferentes ubicaciones geográficas o necesidades de algunos servicios más críticos.

Además, las landing zones también permiten establecer **configuraciones de Alta Disponibilidad** (HA, por sus siglas en inglés) y de **Recuperación ante Desastres** (DR).

- Una **configuración de Alta Disponibilidad** (HA, del inglés High Availability) tiene el propósito de reducir el tiempo de inactividad cuando un recurso, zona o instancia, deja de estar disponible o está dañada. Con la HA, los datos siguen estando disponibles para aplicaciones cliente.

  Por ejemplo una instancia de **Cloud SQL** configurada para HA, también llamada **instancia regional**, se ubica en una zona primaria y una secundaria dentro de la región configurada. Dentro de esta instancia, la configuración se compone de una instancia primaria y

otra en espera. A través de la replicación síncrona a los discos persistentes de cada zona, todas las operaciones de escritura realizadas en la principal se replican en los discos de ambas zonas antes de que una transacción se informe como confirmada. En el caso de un fallo de instancia o de zona, el disco persistente se adjunta a la instancia en espera y se convierte en la nueva instancia principal. Luego, los usuarios son redirigidos a la nueva instancia. Este proceso se denomina conmutación por error.

- Mediante la **Recuperación ante Desastres (DR)** se evita o se mitiga el impacto que pueda tener en el negocio una catástrofe natural, un fallo informático o un ciberataque que pueda causar una interrupción del servicio mayor. En el caso de los servicios de Cloud la idea es poder planear el fallo o indisponibilidad de una región completa.
  - La planificación de recuperación ante desastres comienza con un análisis del impacto en las operaciones, que tiene como objetivo definir dos métricas clave:
    - Un objetivo de tiempo de recuperación (RTO), que es el período máximo aceptable en el que la aplicación puede estar sin conexión. Por lo general, este valor se define como parte de un Acuerdo de Nivel de Servicio (SLA) más amplio.
    - Un objetivo de punto de recuperación (RPO), que es el período máximo aceptable en el que se pueden perder datos de la aplicación debido a un incidente importante. Esta métrica varía según la forma en la que se utilicen los datos. Por ejemplo, los datos del usuario que se modifican con frecuencia podrían tener un RPO de solo algunos minutos. Por el contrario, los datos modificados con menos frecuencia y que resultan menos críticos podrían tener un RPO de varias horas.

Las configuraciones **HA** y **DR** estarán determinadas por el **Objetivo de Nivel de Servicio (SLO)**, que es un elemento medible clave dentro de un **Acuerdo de Nivel de Servicio (SLA).**

Un SLA es el acuerdo completo establecido con un proveedor en el que se especifica qué servicio se proporcionará, cómo se brindará asistencia, los tiempos, las ubicaciones, los costes, el rendimiento, las penalizaciones y las responsabilidades de las partes involucradas. Por su parte, **los SLO son características medibles y específicas del SLA, como la disponibilidad, la capacidad de procesamiento, la frecuencia o el tiempo de respuesta.**

Cabe destacar también **que las landing zones, bajo una nube pública adecuada, permiten que las organizaciones reciban una facturación y reporting perfectamente ajustados**: se pueden establecer métodos de cuotas y límites de servicio con el proveedor, así como la elaboración de informes periódicos con los detalles de los servicios contratados.

Actualmente, prácticamente en todas las industrias a nivel global podemos encontrar múltiples ejemplos de organizaciones que implementan *landing zones* como parte de sus estrategias *cloud*. Además, gran parte de las empresas están implantando estrategias *multi-cloud* y de cloud híbrida para ser más ágiles y eficientes. Por esta razón, estamos viendo ya a muchos clientes plantearse la necesidad de definir una plataforma de autoservicio *cross-cloud* automatizada y definida por código, que a su vez esté integrada con la creación y actualización de las landing zones de los diversos proveedores.

> **Las landing zones, bajo una nube pública adecuada, permiten que las organizaciones reciban una facturación y reporting perfectamente ajustados.**

03
Encuentra los componentes para tu *landing zone*

La cartera de servicios en las grandes nubes públicas suele ser bastante diversa y abarca tres modelos de computación: Infraestructura como Servicio (IaaS), Plataforma como Servicio (PaaS) y Software como Servicio (SaaS). Dichos modelos ofrecen diferentes capas de servicio y ventajas para las organizaciones, de modo que es importante **tener en cuenta las características de cada uno para elegir el que mejor satisfaga las necesidades de la compañía en cuestión:**

- **Infraestructura como Servicio (IaaS):** con un modelo de IaaS, las empresas tienen acceso bajo demanda a recursos de computación escalables como máquinas virtuales. De este modo, se elimina la necesidad de provisionar, configurar o gestionar las infraestructuras y solo se paga por el uso que se hace de estos recursos.
- **Plataforma como Servicio (PaaS)**: este modelo supone dar un paso más arriba en las capas con las que construimos las aplicaciones. Esa "plataforma" nos da un entorno parcialmente gestionado para desplegar las aplicaciones, como puede ser un cluster de contenedores con Kubernetes.
- **Software como Servicio (SaaS):** bajo este modelo se alojan, gestionan y se entregan todas las capas necesarias para una aplicación, típicamente accediendo a ella a través de un navegador web. Ejemplos podrían ser el servicio de correo Gmail, los productos de colaboración de Google Workspace, o alguna de las soluciones de CRM que encontramos en este modelo.

¿DE QUÉ DEPENDE LA ELECCIÓN DE UN MODELO U OTRO?

Cuando una empresa requiere de **un gran control en una aplicación corporativa**, por ejemplo: quiere decidir las versiones o los tiempos de actualización de su *middleware* o de sus sistemas operativos; busca utilizar sus propios aplicativos de operación y gestión; o tiene como objetivo automatizar el despliegue de sus cargas de trabajo actuales sin transformaciones manteniendo sus herramientas de operación, entonces una aproximación **IaaS** será la más conveniente.

Por el contrario, cuando lo que se busca es **desarrollar, producir y escalar una aplicación de forma rápida y a medida de sus necesidades**, un entorno **PaaS** es la mejor solución. Este sería el caso de una organización que, por ejemplo, tenga una aplicación desarrollada en Node.js y busque producirla rápidamente y escalarla de cero a infinito de acuerdo a la demanda de uso de manera inmediata y sin preocuparse de gestionar ningún tipo de infraestructura.

La elección de soluciones **SaaS** será más adecuada cuando se busque implementar aplicaciones comerciales listas para usar, con ciertas capacidades de configuración, pero poca flexibilidad y personalización.

A la hora de crear una landing zone, las organizaciones pueden beneficiarse de estos modelos y obtener así las herramientas o soluciones específicas que necesiten para su migración, ya sea de centros de datos e infraestructura, *middleware*, como los sistemas operativos, o software empresarial listo para ser utilizado desde el principio.

En líneas generales, **los componentes con los que debe contar una *landing zone*** se dividen en las siguientes categorías:

- **Gestión de Identidades y de accesos:** Incluye roles IAM, permisos, cuotas, cuentas de servicio y gestores clave.
- **Jerarquía de la organización:** Define el orden y la estructura de la organización, las carpetas, proyectos y cuentas de facturación.
- **Redes:** Comprende elementos como las subredes, las conexiones a los proveedores *cloud*, la comunicación entre proyectos, los DNS's internos y externos, el direccionamiento de IPs, la comunicación interna de las aplicaciones, así como las reglas de *firewall*.
- **Creación de recursos e instancias.**
- **Almacenamiento:** Incluyendo el cifrado de datos y las claves de ese cifrado.
- **Monitorización:** Comprende los procesos de *logging, alerting*, acceso a *logs* y retenciones.
- **Facturación:** Incluyendo elaboración de informes y definición de cuotas, alertas y cuentas.

04
Hazlo replicable

Una de las principales características de una *landing zone* es su capacidad para ser replicable. Mediante herramientas para crear implementaciones (como Terraform) los desarrolladores pueden mantener un enfoque de Infraestructura como Código (IaC). Esto implica que, en **cada nuevo proyecto, puedan emplear las mismas herramientas que ya utilizaron.**

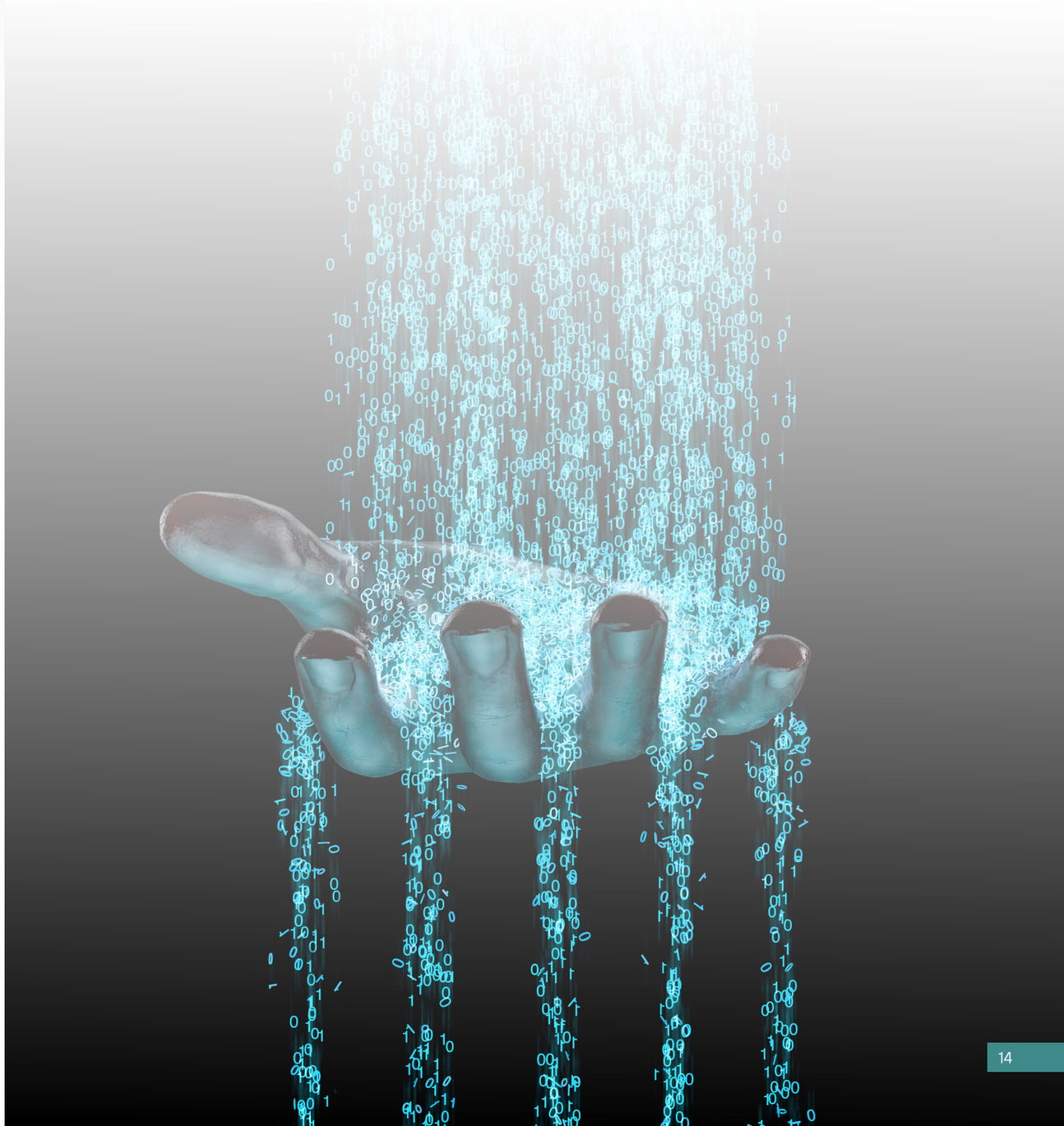
Hashicorp, que creó la Interfaz de Líneas de Comando (CLI) principal de Terraform, desarrolló junto con Google una versión de esta herramienta específica para Google Cloud. Con ella, las organizaciones pueden provisionar recursos de la plataforma con archivos de configuración declarativos, como máquinas virtuales, contenedores, almacenamiento y herramientas de redes. Además, su enfoque IaC es compatible con las prácticas recomendadas de *DevOps* para la administración de cambios.

Esto implica que las organizaciones pueden administrar los archivos de configuración de Terraform en el control de código fuente. Así, les confiere **un estado de aprovisionamiento ideal para entornos de prueba y producción.** Este es el caso de las *landing zones*: de este modo, los proyectos pueden ser fácilmente replicables **y muchas herramientas pueden volver a utilizarse.**

El beneficio más inmediato que pueden obtener los desarrolladores o las organizaciones que replican una *landing zone* para distintos proyectos es la consistencia en todos estos proyectos y sus capas: la nomenclatura de sus elementos, escalabilidad, controles de acceso, entre otros. Esto garantizará una línea de partida segura para evitar configuraciones o políticas no autorizadas en la empresa.

Otro beneficio es la agilidad y rapidez en la creación de nuevos proyectos con nuevas *landing zones*. Al disponer de una semilla de landing zone automatizada, su replicación será prácticamente inmediata y sólo requerirá de personalizaciones en la configuración.

> **En definitiva, las landing zones ofrecen a las organizaciones una gran oportunidad de comenzar su viaje hacia la nube partiendo de una base sólida, con su infraestructura, operaciones y cargas de trabajo segregadas, bajo control, seguras, con una gran flexibilidad y con capacidad para ser replicadas.**



Bibliografía

1. “Gartner: Four Cloudy Predictions”
https://blogs.gartner.com/andrew-lerner/2020/11/10/four-cloudy-predictions/

2. “Gartner: Advanced Cloud Computing Technology”
https://www.gartner.com/en/information-technology/insights/cloud-strategy

3. “Trusted Infraestructure”
https://cloud.google.com/security/infrastructure

4. “Google Cloud Security Foundations Guide”
https://services.google.com/fh/files/misc/google-cloud-security-foundations-guide.pdf

5. “Overview of the high availability configuration”
https://cloud.google.com/sql/docs/mysql/high-availability

6. “What is Disaster Recovery”
https://cloud.google.com/learn/what-is-disaster-recovery

7. “SRE fundamentals 2021: SLIs vs SLAs vs SLOs”
https://cloud.google.com/blog/products/devops-sre/sre-fundamentals-sli-vs-slo-vs-sla

8. “What is IaaS”
https://cloud.google.com/learn/what-is-iaas

9. “App Engine”
https://cloud.google.com/appengine

10. “Software as a service”
https://cloud.google.com/saas

11. “Using Terraform with Google Cloud”
https://cloud.google.com/docs/terraform