GDCD EN AZURE

LIBRO 1



DISEÑO DE CONTRATOS GUIADO POR LA GOBERNANZA

Gobernar Azure por contrato

Guía capa por capa para gobernar una plataforma Azure.

La mayoría de los entornos de Azure no se diseñan. Se acumulan: una suscripción aquí, un rol de Owner allá, un punto de conexión público que nadie recuerda. Esta guía parte del resultado de negocio, lo convierte en garantías y escribe esas garantías como contratos en cada capa de Azure: el inquilino, el árbol de grupos de administración, las suscripciones por entorno, los roles, las directivas, la red, la seguridad, la visibilidad y el costo. El resultado es una zona de aterrizaje gobernada a la que cualquier carga de trabajo, incluidas las de IA, puede incorporarse con seguridad.

Juan Cardena

Arquitecto de IA empresarial y sistemas agénticos · blog.jcardena.com

CONTENIDO

00 Por qué este libro

PARTE I · PRIMERO EL RESULTADO

01 Gobernar antes de construir

02 El inquilino es la primera puerta

PARTE II · LA ESTRUCTURA

03 El árbol de grupos de administración

04 Suscripciones: desarrollo, pruebas, producción y la máquina expendedora

PARTE III · ACCESO Y REGLAS

05 Roles: quién puede hacer qué, y durante cuánto tiempo

06 La directiva es el contrato que se ejecuta

PARTE IV · CAPAS DE GARANTÍA

07 Red: privada de forma predeterminada

08 Una postura de seguridad que se puede observar

09 Visibilidad: un solo lugar para verlo todo

10 Costos: cada número cuadra

PARTE V · OPERAR

11 Implementar por contrato: infraestructura como código

12 El modelo operativo de gobernanza

A Apéndice: Plantillas

ANTES DE EMPEZAR

Por qué este libro



La mayoría de los entornos de Azure no se diseñan. Se acumulan. Un equipo necesita una base de datos, se abre una suscripción fuera de cualquier proceso acordado y, un año después, la organización posee cientos de recursos que nadie puede explicar por completo. Nadie eligió ese resultado. Es simplemente lo que ocurre cuando se empieza a construir antes de gobernar.

Este libro trata de hacerlo al revés. Muestra cómo gobernar un entorno de Azure completo capa por capa: el inquilino (tenant), el árbol de grupos de administración, las suscripciones por entorno, los roles, las directivas, la red, la seguridad, la visibilidad y el costo. Cada capa se trata como una puerta, y cada puerta recibe un contrato: un acuerdo breve, escrito y verificable sobre quién puede cruzar, qué puede cruzar, qué debe ser cierto después y quién se entera.

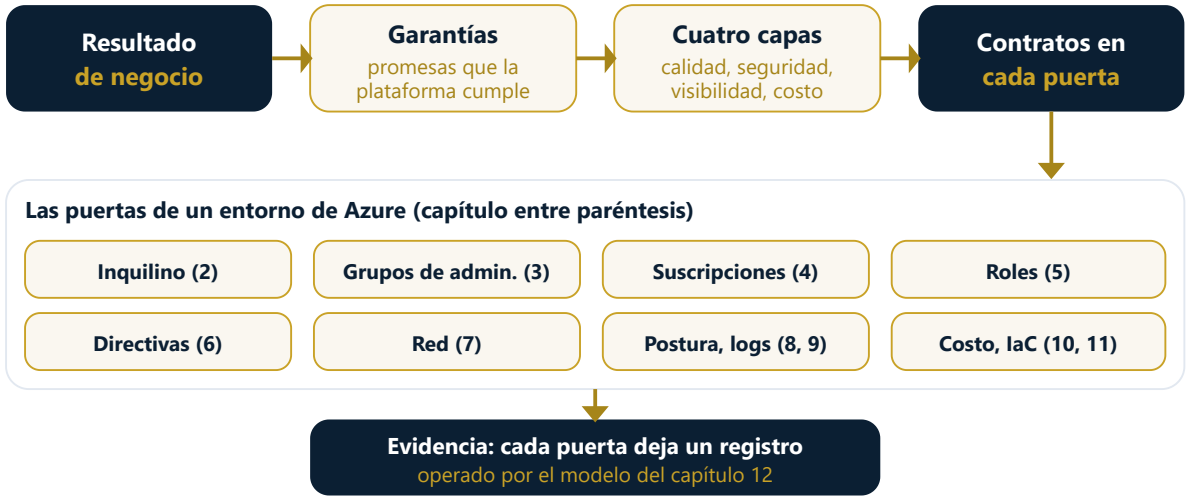
El método que lo sustenta es el Diseño de Contratos Guiado por la Gobernanza (GDCD). El libro fundacional de GDCD, *The Contract Decides: Governing AI at Every Door*, lo presentó para agentes de IA. Este libro aplica la misma columna vertebral a la plataforma en la nube sobre la que se apoyan. En los entornos de producción, no son dos problemas separados. Una carga de trabajo de IA solo está tan gobernada como la suscripción, la identidad y la red en las que se ejecuta.

La columna vertebral del método

GDCD siempre avanza en el mismo orden. Se parte del resultado de negocio. El resultado se convierte en garantías, las promesas que la plataforma debe cumplir. Las garantías se reparten en cuatro capas: calidad, seguridad, visibilidad y costo. Luego, cada garantía se escribe como un contrato en la puerta donde puede hacerse cumplir, y es la plataforma, no la buena voluntad, la que la hace cumplir.

FIGURA 0.1

La columna vertebral de GDCD, aplicada a Azure



Primero el resultado, las puertas al final. Las puertas son los puntos en los que Azure nos permite hacer cumplir las reglas. El libro las recorre en el orden en que un equipo de plataforma debería construirlas.

El orden importa. Los equipos que parten de las herramientas ("necesitamos un firewall", "deberíamos activar Defender") terminan con buenos productos conectados sin ningún propósito. Los equipos que parten del resultado ("los datos de los clientes nunca salen de las regiones aprobadas", "nadie tiene derechos de administrador permanentes en producción") pueden vincular cada configuración con un motivo. Cuando un auditor, un nuevo CISO o un nuevo responsable de plataforma pregunta "¿por qué está esto aquí?", la respuesta ya está escrita.

> *El modelo propone. El contrato decide. En una plataforma en la nube, el "modelo" es toda persona, pipeline o agente que quiera cambiar el entorno.*

Para quién es este libro

Está escrito para las personas responsables de un entorno de Azure: el CIO que firma el presupuesto, el arquitecto de nube que diseña la plataforma, el líder del equipo de plataforma que la opera, el CISO que debe demostrar que es segura y el responsable de FinOps que debe explicar cada línea de la factura. Cada capítulo comienza con su idea central en palabras sencillas, para que un líder pueda leer la primera página y saber qué pedir. El resto del capítulo ofrece el detalle de ingeniería que el equipo de plataforma necesita para llevarlo a cabo.

No necesita leerlo de principio a fin. La estructura sigue el orden en que se construye una plataforma:

Parte	Capítulos	Lo que podrá hacer
I. Primero el resultado	1 a 2	Convertir los resultados de negocio en garantías de plataforma y proteger el inquilino, la primera puerta.
II. La estructura	3 a 4	Dibujar el árbol de grupos de administración y el mapa de suscripciones, y aprovisionar suscripciones gobernadas bajo demanda.
III. Acceso y reglas	5 a 6	Diseñar roles que caducan y escribir directivas que funcionan como un contrato.
IV. Capas de garantía	7 a 10	Hacer que la red sea privada de forma predeterminada, vigilar la postura de seguridad, ver todo en un solo lugar y lograr que cada número cuadre.
V. Operar	11 a 12	Implementar solo mediante código y pipelines, y operar la gobernanza en equipo con un despliegue gradual de 30, 60 y 90 días.
Apéndice	Después del 12	Plantillas: el mapa de grupos de administración y suscripciones, la matriz de roles, el conjunto inicial de directivas, el diccionario de etiquetas y la lista de verificación de preparación.

El principio por encima del producto

Microsoft cambia los nombres de las cosas. Azure Active Directory pasó a ser Microsoft Entra ID. Azure Security Center pasó a ser Microsoft Defender for Cloud. Las herramientas de zonas de aterrizaje (landing zones) se han reconstruido más de una vez. Si este libro enseñara a hacer clic en botones, envejecería en meses. En cambio, cada capítulo enseña primero el patrón y luego muestra cómo Azure lo implementa hoy. El patrón es la parte duradera. El nombre del producto es la dirección actual del patrón.

Cuando el libro menciona un producto, un rol integrado o un efecto de directiva, usa el nombre que figura en la documentación de Microsoft en el momento de redactarlo. Los nombres de productos, los roles integrados y las características se verificaron en la documentación de Microsoft en noviembre de 2026. Las recomendaciones siguen el Microsoft Cloud Adoption Framework y la arquitectura de referencia de zonas de aterrizaje de Azure, porque recogen muchos años de experiencia práctica y porque una plataforma que las sigue es más fácil de traspasar, auditar y mantener. Cuando nos apartamos de la referencia, lo decimos y explicamos por qué.

El libro parte de la nube global de Azure y de un único inquilino corporativo. Las nubes soberanas como Azure Government, los servidores y clústeres fuera de Azure administrados mediante Azure Arc y los entornos operados por un socio mediante Azure Lighthouse siguen

los mismos patrones, pero la disponibilidad de servicios y algunas características difieren, así que consulte la documentación de su nube antes de basarse en un detalle concreto.

> **QUÉ SIGNIFICA "GOBERNADO" EN ESTE LIBRO**
>
> Un entorno está gobernado cuando, para cada suscripción, se pueden responder cinco preguntas en menos de un minuto: quién es su responsable, qué puede contener, quién puede cambiarla y por cuánto tiempo, adónde van sus registros y cuánto puede costar. Cada capítulo añade los controles que hacen que una de esas respuestas sea verdadera y demostrable.

Cómo usar los capítulos

Cada capítulo termina con una breve lista de verificación del contrato: de tres a seis puntos que puede comprobar en su propio entorno. En conjunto, esas listas forman una revisión de preparación que puede realizar sobre un entorno existente. Cada capítulo también remite a una versión interactiva en línea de sus diagramas en hub.jcardena.com/azure, donde puede recorrer el árbol de grupos de administración, el modelo de roles y el conjunto de directivas.

El libro complementario, *AI Foundry by Contract*, construye Microsoft Foundry sobre la plataforma descrita aquí. Si a su organización se le pide entregar IA en Azure, lea primero este libro. Cada barrera de protección de IA del segundo libro presupone el inquilino, el árbol, las suscripciones, los roles y las directivas de este.

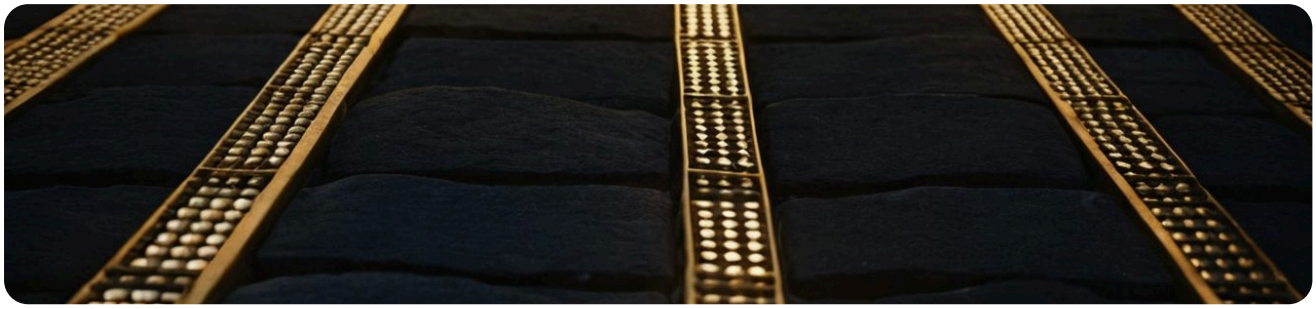
Una promesa recorre cada página: confianza, ganada en cada capa. Una plataforma se gana la confianza del mismo modo que una persona: cumpliendo pequeñas promesas de forma constante y dejando constancia de que lo hizo.

> **LISTA DE VERIFICACIÓN DEL CONTRATO**
>
> - Podemos nombrar los resultados de negocio cuya protección es la razón de ser de nuestra plataforma de Azure.
> - Cada resultado tiene al menos una garantía escrita con un responsable designado.
> - Sabemos qué puerta (inquilino, árbol, suscripción, rol, directiva, red, pipeline) hace cumplir cada garantía.
> - Para cualquier suscripción, podemos indicar el responsable, el contenido, el acceso, los registros y el costo en menos de un minuto.

Véalo en vivo: hub.jcardena.com/azure

CAPÍTULO UNO

Gobernar antes de construir



La gobernanza añadida a posteriori siempre es más cara que la gobernanza diseñada desde el principio. Y no un poco más cara. Cada carga de trabajo construida sin barreras de protección se convierte después en una migración: recursos que mover, permisos que revocar, puntos de conexión públicos que cerrar mientras los usuarios dependen de ellos. El momento más barato para decidir quién puede implementar, dónde pueden residir los datos y cuánto pueden costar las cosas es antes de que exista el primer recurso.

Muchos entornos heredados empezaron al revés. Un proyecto necesitaba resultados rápidos. El equipo obtuvo el rol Owner en una suscripción nueva, construyó algo que funcionaba y pasó a otra cosa. El siguiente equipo copió el patrón. Dos años después hay decenas de suscripciones sin estructura común, registros que se quedan donde nacieron y una factura mensual que nadie puede dividir por producto. El resultado fue consecuencia de la falta de controles de plataforma: la plataforma no tenía contrato, así que cada equipo escribió el suyo.

Por qué se desvían los entornos de Azure

Azure facilita empezar. Eso es una fortaleza. También significa que cada valor predeterminado que usted no cambia se convierte en su norma. Las suscripciones nuevas quedan bajo el grupo de administración raíz del inquilino, a menos que se establezca otro valor predeterminado. Cualquier usuario puede crear un grupo de administración, a menos que se exija autorización para ello. Quien crea una suscripción suele terminar siendo su propietario. Ninguno de estos valores predeterminados es incorrecto para un solo equipo. Todos son incorrectos para una empresa, y se acumulan en silencio.

La desviación tiene tres caras que los líderes reconocen:

- **Desviación del acceso.** Las asignaciones de Owner y Contributor se acumulan en personas individuales, en ámbitos amplios y sin fecha de finalización. Nadie recuerda por qué existe la mitad de ellas.
- **Desviación de la configuración.** Una carga de trabajo usa puntos de conexión privados, la siguiente expone una cuenta de almacenamiento a Internet, y ambas superaron su propia revisión.
- **Desviación del costo.** El gasto crece más rápido de lo que cualquier responsable puede explicar, porque los recursos no llevan etiqueta de responsable, centro de costo ni entorno.

Cada una de ellas es una promesa rota en la que el negocio nunca supo que confiaba. GDCD nombra primero esa promesa y luego hace que la plataforma la cumpla.

Del resultado a la garantía, y de la garantía al mecanismo que la hace cumplir

El método de este libro comienza con una breve conversación con el negocio, no con una lista de productos. ¿Qué no debe ocurrir nunca? ¿Qué debe ser cierto siempre? ¿Qué debemos poder demostrar? Las respuestas son resultados de negocio. Después reescribimos cada uno como una garantía: una afirmación precisa que la plataforma puede cumplir. Por último, nombramos el mecanismo de aplicación: la función de Azure que hace cumplir la garantía sin depender de la memoria de nadie.

FIGURA 1.1

Cuatro resultados, vinculados a la puerta de Azure que los hace cumplir



Una fila sin mecanismo de aplicación es un deseo. Márquela o elimínela.

Léalo de izquierda a derecha en la reunión y de derecha a izquierda en la auditoría. La primera columna corresponde a los líderes. La tercera, al equipo de plataforma. La garantía del centro es el contrato entre ambos.

Observe que ninguna de las garantías menciona un producto. "Ningún recurso se crea fuera de la lista de regiones" seguirá siendo la garantía correcta si el mecanismo de aplicación cambia de nombre o se sustituye. Es la regla del prefacio, el principio por encima de la herramienta, aplicada a una decisión real.

Las cuatro capas de garantía

Una vez escritos los resultados, clasifique las garantías en las cuatro capas que recorren toda la serie GDCD. Cada capa tiene una unidad mínima y un fallo silencioso que no tolera.

Capa	Qué garantiza en Azure	El fallo silencioso que no tolera	Capítulos
Calidad	Los cambios llegan mediante código y pipelines probados, y la promoción de desarrollo a pruebas y a producción es repetible.	Una corrección manual en producción que nadie puede reproducir.	4, 11
Seguridad	Las identidades son robustas, el acceso es mínimo y temporal, y las redes son privadas de forma predeterminada.	Un Owner olvidado o un punto de conexión público que nadie eligió.	2, 5, 7, 8

Visibilidad	Cada suscripción envía sus registros a un solo lugar, y cada alerta llega a una persona.	Un evento que ocurrió pero no dejó ningún registro que alguien pudiera encontrar.	9
Costo	Cada recurso tiene un responsable y un centro de costo, y cada suscripción tiene un presupuesto.	La línea de la factura que nadie puede explicar.	10

Los contratos, es decir, las reglas de directivas y roles de la Parte III, no son una quinta capa. Son la forma de hacer cumplir las cuatro capas. Por eso este libro dedica dos capítulos completos a los roles y las directivas antes de llegar a la red.

Qué significa realmente "antes de construir"

Gobernar primero no significa una fase de diseño de seis meses antes de que nadie pueda implementar. Ese enfoque fracasa de otra manera: los equipos sortean la plataforma porque todavía no existe. Lo que funciona en la práctica es primero una base mínima cuyas reglas se hacen cumplir, y luego una entrega rápida sobre ella.

1. **Proteger el inquilino** (capítulo dos): cuentas de acceso de emergencia, autenticación sólida e identidades de administrador separadas.
2. **Dibujar el árbol** (capítulo tres): grupos de administración que reflejan los tipos de carga de trabajo, no el organigrama.
3. **Abrir la máquina expendedora** (capítulo cuatro): un formulario de solicitud que produce una suscripción gobernada con responsable, etiquetas, presupuesto y red ya establecidos.
4. **Vincular el acceso y las reglas** (capítulos cinco y seis): roles asignados a grupos y convertidos en temporales, y un conjunto inicial de directivas que se ejecuta primero en modo de auditoría y luego se hace cumplir.

Esa base es deliberadamente pequeña. Las capas de garantía de la Parte IV y el modelo operativo de la Parte V la refuerzan con el tiempo. Lo que importa es que la primera carga de trabajo llegue a una suscripción gobernada, para que la segunda y la número cincuenta también lo hagan.

UN ENTORNO HEREDADO HABITUAL

Un equipo de plataforma hereda un entorno con muchas suscripciones, la mayoría situadas directamente bajo la raíz del inquilino. El equipo no empieza moviendo nada. Primero crea el árbol de grupos de administración, establece Sandbox como grupo de administración predeterminado para las suscripciones nuevas y asigna un pequeño conjunto de directivas en modo de auditoría en la parte superior del árbol y directamente a las suscripciones existentes, hasta que estas se trasladen al árbol. En pocos días, la vista de cumplimiento muestra exactamente dónde está la deuda. El entorno no cambió, pero por primera vez pudo medirse. El capítulo doce convierte ese primer paso en un despliegue gradual de 30, 60 y 90 días.

No gobierne solo con documentos. Una página de wiki que dice "implemente solo en regiones aprobadas" es un deseo. Una asignación de directiva con el efecto Deny en el grupo de administración de zonas de aterrizaje es un contrato. Escriba el documento para las personas y asegúrese de que cada regla que contiene nombre su mecanismo de aplicación.

El costo de gobernar tarde

No damos una cifra universal, porque depende del entorno. El patrón, sin embargo, es constante. La gobernanza tardía llega en forma de tres facturas separadas: una por construir sin barreras de protección, otra por averiguar qué se construyó y otra por corregirlo mientras funciona en producción con usuarios que dependen de ello. La gobernanza temprana se paga una vez, y la mayor parte de ese costo es automatización que el equipo de plataforma reutiliza para cada carga de trabajo posterior.

> *Las barreras de protección son más baratas antes de que exista el primer recurso. Después, cada una de ellas es una migración.*

También hay un costo que nunca aparece en una factura: la confianza. Cuando un CISO no puede decir quién tiene derechos de administrador en producción, o un CFO no puede decir qué producto impulsó el gasto del mes pasado, la confianza en todo el programa de nube cae. Una plataforma gobernada responde a esas preguntas en minutos. Ese es el verdadero resultado de negocio de todo lo que sigue. Confianza, ganada en cada capa.

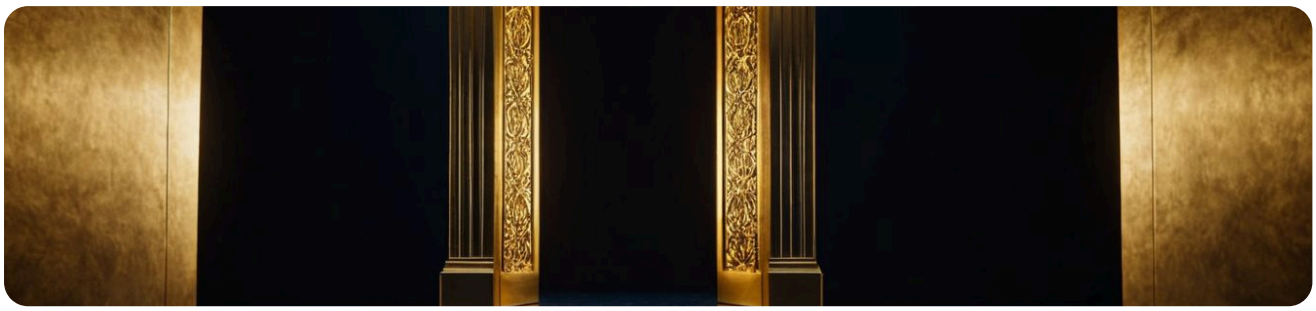
LISTA DE VERIFICACIÓN DEL CONTRATO

- Hemos escrito de tres a seis resultados de negocio para la plataforma y los hemos acordado con sus responsables.
- Cada resultado está reescrito como una garantía independiente del producto.
- Cada garantía nombra un mecanismo de aplicación de Azure y el capítulo que lo construye, o está marcada como un deseo.
- Hemos establecido un grupo de administración predeterminado para las suscripciones nuevas, de modo que ninguna quede bajo la raíz del inquilino.
- Tenemos un plan de base mínima (inquilino, árbol, aprovisionamiento, roles, directivas) antes de incorporar la siguiente carga de trabajo.

Véalo en vivo: el mapa de gobernanza en hub.jcardena.com/azure/governance.html

CAPÍTULO DOS

El inquilino es la primera puerta



Toda acción en Azure comienza con un inicio de sesión. Antes de que alguien toque una suscripción, una directiva o una red, Microsoft Entra ID ya ha decidido quién es y con qué grado de certeza. Si esa decisión es débil, nada de lo que se construya encima puede ser sólido. El inquilino es la primera puerta, y es la puerta en la que confían todas las demás.

Un inquilino (tenant) de Microsoft Entra es el límite de identidad de la organización. Cada suscripción confía exactamente en un inquilino, y el árbol de grupos de administración del capítulo tres reside dentro de él. Todas las suscripciones de un grupo de administración deben confiar en el mismo inquilino. Por eso la primera decisión de plataforma no trata en absoluto de recursos de Azure. Trata de cuántos inquilinos tiene y de con qué solidez se autentica cada identidad dentro de ellos.

Un solo inquilino, salvo que un requisito obligue a tener más

La guía de zonas de aterrizaje de Microsoft es clara: use un único inquilino de Microsoft Entra, normalmente el inquilino corporativo donde las personas ya inician sesión para el correo y la colaboración, y cree más inquilinos solo cuando un requisito no pueda cumplirse en el corporativo. Las razones son prácticas. Las zonas de aterrizaje de Azure se implementan por inquilino, así que cada inquilino adicional significa otro árbol, otro conjunto de directivas y otro conjunto de registros. Las licencias de Microsoft Entra ID P1 o P2 no abarcan varios inquilinos. Muchos servicios de Azure se integran de forma nativa con las identidades de su inquilino de origen y ofrecen compatibilidad limitada con invitados de otros inquilinos.

La separación dentro de un mismo inquilino se logra con estructura, no con más inquilinos: grupos de administración y suscripciones para los recursos, y unidades administrativas para delegar la administración de usuarios y grupos. Las suscripciones de Sandbox dan a los

equipos espacio para experimentar sin un inquilino de "pruebas" separado para Azure. Un inquilino dedicado a probar la propia configuración de identidad puede seguir teniendo sentido, pero no debería alojar cargas de trabajo de Azure.

> **Mover suscripciones entre inquilinos no es una solución rápida.** Transferir una suscripción a otro directorio elimina las asignaciones de roles existentes y exige un trabajo cuidadoso antes y después. Microsoft señala que a menudo es más fácil reconstruir la carga de trabajo en una suscripción nueva del inquilino de destino. Decida el inquilino antes de construir, no después.

Cuatro tipos de identidad, cuatro contratos

Dentro del inquilino, separamos las identidades según su finalidad, porque cada tipo necesita un contrato distinto. Mezclarlas es una de las debilidades de identidad más comunes en los entornos heredados.

FIGURA 2.1

La puerta del inquilino: cada identidad pasa por la misma entrada, con su propio contrato



Discontinua: cuentas de emergencia exentas del bloqueo condicional; alerta en cada uso.

Una entrada, cuatro contratos. La entrada es la misma para todos. Lo que cambia es con qué solidez se autentica cada identidad, qué roles puede tener y cómo se vigila su uso.

Identidad	Contrato
Cuenta diaria	No tiene roles administrativos en Entra ni en Azure. Está protegida por autenticación multifactor y acceso condicional, como cualquier usuario.
Cuenta de administración	Una cuenta separada, solo en la nube, usada únicamente para administración. Tiene asignaciones de roles aptas (eligible) en Privileged Identity Management y

	activa los roles cuando los necesita. Usa autenticación resistente al phishing.
Acceso de emergencia	Dos o más cuentas solo en la nube, en el dominio onmicrosoft.com, con autenticación mediante clave de paso (FIDO2) o basada en certificados. Nunca se usan en el día a día y generan una alerta en cada inicio de sesión.
Identidad de carga de trabajo	Identidades administradas para los recursos de Azure y credenciales federadas para los pipelines. Sin contraseñas compartidas y sin cuentas de usuario que actúen como cuentas de servicio.

La autenticación sólida ya no es opcional

Microsoft ahora hace obligatoria la autenticación multifactor para los inicios de sesión en Azure. En la primera fase, las cuentas que inician sesión en Azure Portal, el Centro de administración de Microsoft Entra y el Centro de administración de Intune deben completar MFA. En la segunda fase, las cuentas que crean, actualizan o eliminan recursos mediante la CLI de Azure, Azure PowerShell, herramientas de infraestructura como código, SDK y la API REST también deben completar MFA. Las identidades de carga de trabajo, como las identidades administradas y las entidades de servicio, no se ven afectadas. Las cuentas de usuario usadas como cuentas de servicio sí, lo cual es una razón más para retirarlas.

La MFA obligatoria es un mínimo, no un diseño. El contrato de un inquilino empresarial va más allá: directivas de acceso condicional que exigen MFA a todos los usuarios, métodos resistentes al phishing para los administradores y el bloqueo de la autenticación heredada. El acceso condicional requiere Microsoft Entra ID P1 o P2. Los inquilinos que no lo tengan deberían al menos activar los valores predeterminados de seguridad.

Las identidades de carga de trabajo no pueden realizar MFA, por lo que su contrato en la puerta del inquilino es distinto. El acceso condicional para identidades de carga de trabajo puede bloquear una entidad de servicio de un solo inquilino cuando solicita un token desde fuera de los intervalos de IP conocidos, o cuando Microsoft Entra ID Protection la califica como de riesgo. Requiere licencias de Workload Identities Premium y no abarca las identidades administradas, que no tienen ninguna credencial que alguien almacene o manipule. Para las personas, ID Protection con Microsoft Entra ID P2 aporta el riesgo de usuario y de inicio de sesión al acceso condicional, de modo que un inicio de sesión de riesgo puede bloquearse o requerir un cambio seguro de contraseña.

Acceso de emergencia: la puerta para el peor día

Todo control sólido puede dejarlo sin acceso. Una interrupción de la federación, una directiva de acceso condicional mal configurada o la salida de todos los aprobadores pueden hacer que nadie pueda administrar el inquilino. Las cuentas de acceso de emergencia (break-

glass) existen para ese día. La guía de Microsoft es específica, y la seguimos tal como está escrita:

- Al menos dos cuentas, solo en la nube, en el dominio onmicrosoft.com, ni federadas ni sincronizadas.
- Autenticación mediante clave de paso (FIDO2) o basada en certificados, distinta de los métodos que usan los administradores habituales.
- Rol Administrador global con asignación activa permanente en PIM, no apta.
- Excluidas, mediante un grupo dedicado, de las directivas de acceso condicional que bloquean o restringen el inicio de sesión.
- Credenciales almacenadas en ubicaciones seguras separadas y usadas desde una estación de trabajo segura.
- Cada inicio de sesión genera una alerta, y las cuentas se validan al menos cada 90 días.

Es la alerta lo que convierte una cuenta de emergencia, de riesgo oculto, en una puerta gobernada. Envíe los registros de inicio de sesión de Entra al área de trabajo central de Log Analytics (capítulo nueve) y cree una regla de alertas de registro que se active ante cualquier resultado:

```
// Cualquier inicio de sesión de una cuenta de acceso de emergencia genera una alerta crítica
SigninLogs
| where UserId == "<object-id-1>" or UserId == "<object-id-2>"
| project TimeGenerated, UserPrincipalName, UserId, IPAddress, ResultType, ResultDescription
```

> **EL SIMULACRO QUE REVELA LO QUE FALTA**
>
> Un simulacro trimestral de acceso de emergencia funciona mejor como un evento de calendario con dos personas presentes. Una inicia sesión y la otra vigila que llegue la alerta. El simulacro detecta con regularidad desviaciones que ningún otro control detectaría: una directiva de acceso condicional añadida sin el grupo de exclusión, o un grupo de acciones de alerta que apunta a un buzón que ya no existe.

Limite las asignaciones del rol más poderoso

El rol Administrador global controla el inquilino, y un administrador global puede elevar su acceso para administrar todas las suscripciones y grupos de administración de Azure. Microsoft recomienda reducir al mínimo las asignaciones de Administrador global (preferiblemente menos de cinco), configurar los roles de administración como aptos en PIM, exigir aprobación para activar los más críticos y notificar cada activación a las partes

interesadas. Use los roles de Entra más específicos para el trabajo diario. La opción "Administración de acceso para recursos de Azure" debe permanecer desactivada para los administradores globales que no la necesiten, porque concede el rol User Access Administrator en la raíz del árbol.

Dispositivos de administración y consentimiento de aplicaciones

Un inicio de sesión sólido no sirve de nada en un dispositivo comprometido. Los administradores del inquilino y de la plataforma trabajan desde estaciones de trabajo de acceso privilegiado: dispositivos reforzados y administrados que se usan solo para administración, y que el acceso condicional puede exigir para los roles de administración mediante el cumplimiento de dispositivos. Las aplicaciones son la otra vía silenciosa de entrada al inquilino. Restrinja el consentimiento de los usuarios, por ejemplo a editores verificados y permisos de bajo riesgo, o desactívelo, y active el flujo de trabajo de consentimiento del administrador para que los usuarios puedan solicitar aprobación en lugar de eludir el bloqueo. Decida quién puede crear registros de aplicaciones, porque de forma predeterminada cualquier usuario miembro puede hacerlo, y asigne a cada registro un propietario designado.

> *Cada puerta por encima del inquilino confía en el inquilino. Haga que la primera puerta sea la más fuerte.*

LISTA DE VERIFICACIÓN DEL CONTRATO

- Todas las suscripciones de Azure confían en un único inquilino corporativo, y cada inquilino adicional tiene un requisito por escrito.
- Los administradores usan cuentas de administración separadas, solo en la nube, con autenticación resistente al phishing.
- Existen dos o más cuentas de acceso de emergencia, excluidas de las directivas de acceso condicional que bloquean, y generan una alerta en cada inicio de sesión.
- El simulacro de acceso de emergencia se ha realizado en los últimos 90 días.
- El rol Administrador global tiene menos de cinco asignaciones, todas aptas en PIM, excepto las de las cuentas de emergencia.
- Ninguna cuenta de usuario se usa como cuenta de servicio para la automatización.

Véalo en vivo: el mapa de roles en hub.jcardena.com/azure/governance-roles.html

PARTE II · LA ESTRUCTURA

CAPÍTULO TRES

El árbol de grupos de administración



Un árbol de grupos de administración es un organigrama del riesgo, no de las personas. Cada rama contiene suscripciones que necesitan las mismas reglas, y cada regla asignada a una rama se hereda hacia todo lo que está debajo. Dibuje el árbol en función de lo que necesitan las cargas de trabajo, manténgalo poco profundo, y la mayor parte del diseño de directivas y accesos encajará por sí sola.

Los grupos de administración son el ámbito de gobernanza situado por encima de las suscripciones. Las asignaciones de directivas y de roles realizadas en un grupo de administración las heredan todos los grupos de administración secundarios, suscripciones, grupos de recursos y recursos. Esa herencia es justamente el objetivo. Una sola asignación en la rama correcta sustituye a cientos de configuraciones por suscripción, y nadie por debajo de la rama puede quedar fuera sin que se note.

Los hechos que condicionan el diseño

Algunos hechos de la plataforma, tomados de la documentación de Microsoft, fijan los límites de cualquier árbol:

- Cada directorio tiene un grupo de administración raíz, que se muestra de forma predeterminada como **Grupo raíz del inquilino** y cuyo identificador es el identificador del inquilino. No se puede mover ni eliminar.
- Un árbol admite hasta seis niveles de profundidad, sin contar la raíz ni el nivel de suscripción.
- Cada grupo de administración, salvo la raíz, y cada suscripción tienen exactamente un elemento primario.
- Las suscripciones nuevas quedan bajo el grupo de administración raíz, a menos que se establezca un grupo de administración predeterminado, como se describe más adelante.

- De forma predeterminada, cualquier entidad de seguridad del inquilino puede crear grupos de administración, a menos que se exija autorización en la configuración de la jerarquía.

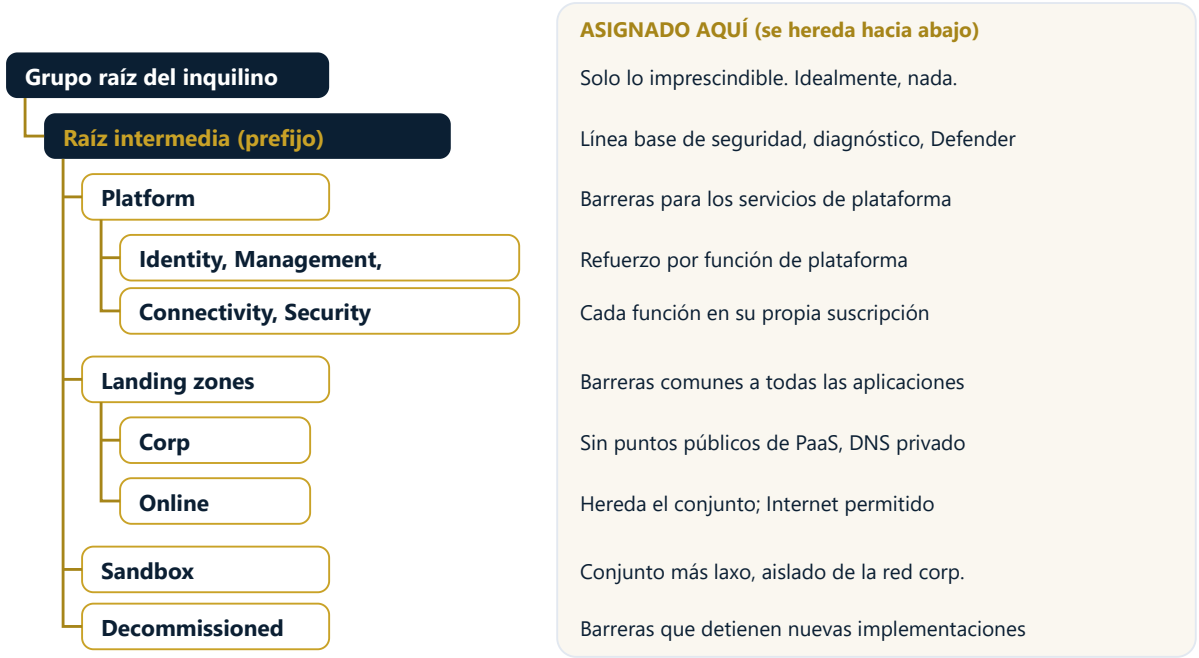
Los seis niveles son un límite, no un objetivo. El Cloud Adoption Framework recomienda mantener la jerarquía razonablemente plana, idealmente con un máximo de tres o cuatro niveles. Cada nivel adicional es un lugar más donde una regla heredada puede sorprender a alguien.

El árbol de la zona de aterrizaje

La arquitectura de referencia de zonas de aterrizaje de Azure ofrece un árbol que se adapta a la mayoría de las empresas con pocos cambios. Nuestro equipo de plataforma parte de él en cada árbol nuevo, porque recoge la experiencia práctica y porque el próximo ingeniero de plataforma lo reconocerá.

FIGURA 3.1

El árbol de la zona de aterrizaje de Azure y lo que se asigna en cada nivel



Izquierda: el árbol. Derecha: el contrato de cada rama. Las suscripciones de cargas de trabajo residen bajo Corp u Online. Las suscripciones de plataforma residen bajo su grupo de plataforma. Sandbox y Decommissioned se sitúan directamente bajo la raíz intermedia. Cuando sea necesario, puede añadirse un grupo Local bajo Landing zones para cargas de trabajo híbridas de Azure Local.

Cada grupo tiene una función clara:

Grupo de administración	Contiene	Propósito de sus reglas
Raíz intermedia	Todo lo que está debajo, con un nombre que lleva el prefijo de la organización	Permite no asignar nada en la raíz del inquilino y ofrece un único nivel superior para la línea base del entorno.
Platform	Los grupos Identity, Management, Connectivity y Security	Cada uno contiene una suscripción dedicada: servicios de identidad, el área de trabajo central de Log Analytics, la red hub y herramientas de seguridad como Microsoft Sentinel.
Landing zones	Corp, Online y, opcionalmente, Local	Corp es para las cargas de trabajo que se conectan a la red corporativa a través del hub. Online es para las cargas de trabajo que necesitan acceso directo a Internet o que no usan ninguna red virtual.
Sandbox	Suscripciones de experimentación	Un conjunto de directivas menos restrictivo para la exploración, aislado de las zonas de aterrizaje Corp y Online.
Decommissioned	Zonas de aterrizaje canceladas	Zona de espera para las suscripciones en proceso de retirada, con barreras de protección que impiden un nuevo uso.

Las asignaciones de directivas predeterminadas de los aceleradores de zonas de aterrizaje de Azure siguen esta estructura. En el momento de redactar este libro, por ejemplo, el grupo Corp tiene una asignación con el efecto Deny que deshabilita el acceso a la red pública para los servicios PaaS, y Sandbox y Decommissioned tienen cada uno su propia iniciativa de barreras de protección. La lista exacta evoluciona con cada versión, así que trate las asignaciones actuales del acelerador como un punto de partida que revisar, no como un estándar fijo.

Reglas para un árbol que perdure

REGLAS DE DISEÑO QUE APLICAMOS

- **Agrupe por arquetipo de carga de trabajo, no por departamento.** Los departamentos se reorganizan. Las reglas que necesita una carga de trabajo conectada a la red corporativa, no.
- **No cree grupos de administración para desarrollo, pruebas y producción.** Los entornos son suscripciones separadas dentro del mismo grupo de arquetipo. El capítulo cuatro explica por qué, y el capítulo seis trata la parte de las directivas.
- **No cree grupos de administración por región**, salvo que lo exija un requisito legal basado en la ubicación, como la residencia de datos.
- **Asigne directivas en los grupos de administración y accesos en las suscripciones.** Los equipos de cargas de trabajo reciben roles en el ámbito de suscripción o de grupo de recursos. Los equipos de plataforma pueden tener roles en el ámbito de grupo de administración, controlados mediante PIM.
- **Mantenga la raíz casi vacía.** Todo lo que se asigna en la raíz del inquilino se aplica a todos los recursos del directorio.
- **Use etiquetas, no profundidad, para las vistas transversales.** El centro de costo o el producto pueden consultarse en todo el árbol sin añadir niveles.

Vale la pena mostrar la aritmética de la segunda regla a quien quiera grupos por entorno. Treinta cargas de trabajo, cada una con su propio grupo más grupos secundarios para desarrollo, pruebas y producción, producen 120 grupos de administración. Es el ejemplo que Microsoft usa en su propia guía, y cada uno de esos grupos es un lugar donde las reglas pueden divergir entre entornos.

Proteja el propio árbol

El árbol es un contrato, así que sus cambios necesitan sus propias barreras de protección. Dos opciones de configuración de la jerarquía importan desde el primer día. Primero, exija autorización para las operaciones de grupos de administración, de modo que solo las entidades de seguridad con el permiso adecuado de Azure RBAC puedan crear grupos. Segundo, establezca un grupo de administración predeterminado para las suscripciones nuevas. Microsoft sugiere el grupo Sandbox como buen candidato, para que cualquier suscripción nueva llegue con un conjunto de directivas ya aplicado en lugar de quedar bajo la raíz sin ninguno.

Construya el árbol mediante código, como todo lo demás (capítulo once). Un grupo de administración es un recurso pequeño que se implementa en el ámbito del inquilino:

```
targetScope = 'tenant'

param prefix string = 'org'

resource landingZones 'Microsoft.Management/managementGroups@2021-04-01' = {
  name: '${prefix}-landingzones'
  properties: {
    displayName: 'Landing zones'
    details: {
      parent: {
        id: tenantResourceId('Microsoft.Management/managementGroups', prefix)
      }
    }
  }
}
```

Los traslados importan tanto como la creación. Trasladar una suscripción entre ramas cambia qué directivas se le aplican, y Azure Resource Manager puede almacenar en caché los detalles de la jerarquía hasta 30 minutos, por lo que el portal puede tardar en reflejar un traslado. Los traslados los realiza el equipo de plataforma mediante el pipeline, nunca a mano, y cada traslado es visible en el registro de actividad en el ámbito del grupo de administración.

TRASLADAR UN ENTORNO HEREDADO AL ÁRBOL

Cuando una suscripción existente pasa de la raíz a Corp, de repente hereda un Deny sobre los puntos de conexión públicos. Los recursos existentes siguen funcionando y aparecen como no conformes, y el siguiente cambio sobre ellos se deniega. Microsoft también documenta casos en los que la directiva bloquea el propio traslado debido a propiedades de los recursos dentro de la suscripción. Por eso solo trasladamos suscripciones después de que el conjunto de directivas se haya ejecutado en modo de auditoría sobre ellas y los responsables tengan un plan, o después de que cada Deny de la rama de destino se haya establecido en DoNotEnforce, de modo que el traslado cambie lo que se mide, no lo que se permite. Cuando el traslado deba hacerse primero, una exención temporal con fecha de expiración cubre la transición; para el caso del traslado bloqueado, puede crearse una exención antes del traslado con la validación del ámbito de asignación establecida en DoNotValidate, una opción en versión preliminar en el momento de redactar este libro. El capítulo seis muestra cómo funcionan las exenciones.

> *Dibuje el árbol una vez, en torno al riesgo. Después deje que la herencia haga el trabajo repetitivo, cada minuto, sin que nadie tenga que acordarse.*

LISTA DE VERIFICACIÓN DEL CONTRATO

- Nuestro árbol sigue la estructura de la zona de aterrizaje: raíz intermedia, Platform, Landing zones, Sandbox, Decommissioned.
- El árbol no tiene más de cuatro niveles por debajo de la raíz, ni ramas por entorno o departamento.
- No se asigna nada en la raíz del inquilino sin un motivo escrito que lo haga imprescindible.
- La creación de grupos de administración requiere autorización, y las suscripciones nuevas van a Sandbox de forma predeterminada.
- El árbol se implementa y se modifica solo mediante código.

Véalo en vivo: el mapa de la zona de aterrizaje en hub.jcardena.com/azure/governance-landing-zone.html

CAPÍTULO CUATRO

Suscripciones: desarrollo, pruebas, producción y la máquina expendedora



La suscripción es la unidad de control en Azure. Es donde se concede el acceso, donde se fija un presupuesto, donde se aplican las cuotas y donde se reparte la factura. Asigne a cada carga de trabajo una suscripción por entorno, colóquelas en la rama correcta del árbol y deje que una máquina expendedora las cree. Así, cada nueva carga de trabajo nace gobernada, en minutos, sin una cola de tickets.

El Microsoft Cloud Adoption Framework llama a esto democratización de suscripciones: las suscripciones, no los grupos de recursos, son la unidad principal de administración y escalado de las cargas de trabajo. Esa decisión tiene un beneficio directo para la gobernanza. Una suscripción es un límite sólido para el acceso, la facturación, las cuotas y las implementaciones. El acceso concedido dentro de una suscripción no alcanza a otra, una alerta de presupuesto nombra a un solo responsable, y un error en desarrollo no puede tocar un recurso de producción que ni siquiera ve. Solo dos cosas cruzan ese límite a propósito: los roles heredados de un grupo de administración y las rutas de red construidas entre suscripciones.

Una suscripción por carga de trabajo y por entorno

Según la guía de Microsoft, lo ideal es que cada entorno de una aplicación tenga su propia suscripción. Desarrollo, pruebas y producción de la misma carga de trabajo se convierten en tres suscripciones, todas ubicadas en el mismo grupo de administración de arquetipo, Corp u Online. Sandbox es la única excepción: el trabajo exploratorio se ubica en suscripciones del grupo Sandbox, con un conjunto de directivas más flexible y sin ninguna ruta hacia la red corporativa.

FIGURA 4.1

Un mapa de suscripciones: los entornos son suscripciones, no ramas

Carga de trabajo	Grupo de arquetipo	Desarrollo	Pruebas	Producción
Portal de reclamaciones	Corp	sub-claims-dev	sub-claims-test	sub-claims-prod
Sitio web público	Online	sub-web-dev	sub-web-test	sub-web-prod
Plataforma de datos	Corp	sub-data-dev	sub-data-test	sub-data-prod
Experimentos de equipo	Sandbox	sub-sbx-<team>, por tiempo limitado, sin conectividad corporativa		

Mismo grupo, mismas barreras de protección, radio de impacto separado. Cada fila avanza de un entorno a otro con reglas idénticas, de modo que lo que se valida en pruebas se comporta igual en producción. El límite de la suscripción mantiene un error de desarrollo fuera de producción.

¿Por qué no usar grupos de administración para cada entorno? Porque la guía de Microsoft, y nuestra experiencia, indican que los entornos del ciclo de desarrollo no deben tener barreras de protección distintas. Si desarrollo permite una cuenta de almacenamiento pública y producción la deniega, el equipo descubre el problema solo en el último paso, después de haber construido sobre el diseño equivocado. Mantenga iguales las barreras de protección y deje que el límite de la suscripción aporte el aislamiento. Cuando producción realmente necesite una obligación adicional, como la copia de seguridad, agréguela en el ámbito de la suscripción durante el aprovisionamiento.

Existen excepciones legítimas. Algunos diseños comparten un único recurso entre entornos, y las ranuras de implementación de App Service son un ejemplo común, porque una ranura reside en un solo plan de App Service dentro de una sola suscripción. La guía de Microsoft permite una única suscripción para varios entornos cuando no pueden aislarse, comparten los mismos operadores y pueden usar las mismas directivas. Deje constancia escrita de la excepción y protéjala con acceso en el ámbito del grupo de recursos a través de PIM.

La máquina expendedora

El aprovisionamiento de suscripciones (subscription vending) es el mecanismo de la plataforma que entrega suscripciones gobernadas a petición. Ofrece a los equipos de carga de trabajo una única puerta de entrada oficial, da al equipo de plataforma el control del

estado inicial de cada suscripción y sustituye semanas de tickets por una ejecución del pipeline. Participan tres equipos: el Centro de Excelencia en la Nube (CCoE) define las reglas de negocio y la lógica de aprobación, el equipo de carga de trabajo hace la solicitud, y la automatización del equipo de plataforma crea y configura la suscripción antes de entregarla.

FIGURA 4.2

Aprovisionamiento de suscripciones: de la solicitud a una suscripción gobernada



La solicitud es el contrato. Todo lo que pide el formulario se convierte en un parámetro, y cada parámetro se convierte en una garantía que la suscripción lleva consigo desde su primer minuto.

En el formulario de solicitud, la gobernanza resulta económica. Microsoft recomienda recopilar en la solicitud el presupuesto previsto, los responsables de la suscripción, las expectativas de red, la criticidad para el negocio y la clasificación de confidencialidad. Esas respuestas deciden la ubicación en el árbol, la forma de la red, el presupuesto y quién aprueba. Integre el formulario con su herramienta actual de administración de servicios de TI, para que las aprobaciones, el historial de auditoría y los informes vivan donde la organización ya los busca, y use una herramienta de administración de direcciones IP para que no se solapen los espacios de direcciones de las redes spoke.

Hay tres detalles fáciles de pasar por alto. Primero, la solicitud debe indicar si la carga de trabajo es Production o DevTest, porque la oferta Dev/Test tiene tarifas más bajas para algunos recursos pero condiciones diferentes, y no está disponible en todos los tipos de acuerdo de facturación. Segundo, las cuotas se aplican por suscripción y por región, por ejemplo las vCPU por familia de máquinas virtuales, de modo que una suscripción nueva empieza con los límites predeterminados. El formulario debe solicitar la escala prevista, y el pipeline de aprovisionamiento debe solicitar los aumentos de cuota que la carga de trabajo

necesita antes de la entrega, para que la primera implementación en producción no quede bloqueada por un límite. Tercero, los presupuestos son alertas, no límites estrictos. El presupuesto creado durante el aprovisionamiento avisa a los responsables cuando el gasto se acerca al umbral; no detiene los recursos. El capítulo diez trata los controles que sí lo hacen.

El aprovisionamiento como código

Microsoft publica módulos de aprovisionamiento de suscripciones para Bicep y Terraform como Azure Verified Modules. El pipeline, ejecutado desde GitHub Actions o Azure Pipelines con una identidad de carga de trabajo federada, llama al módulo con los parámetros de la solicitud aprobada. Un ejemplo abreviado en Bicep:

```
targetScope = 'managementGroup'

// Nombres de parámetros tal como se publicaron para la versión 0.8.0 del módulo.
module claimsProd 'br/public:avm/ptn/lz/sub-vending:0.8.0' = {
  name: 'vend-claims-prod'
  params: {
    subscriptionAliasEnabled: true
    subscriptionAliasName: 'sub-claims-prod'
    subscriptionDisplayName: 'sub-claims-prod'
    subscriptionBillingScope: billingScope
    subscriptionWorkload: 'Production'
    subscriptionManagementGroupAssociationEnabled: true
    subscriptionManagementGroupId: 'org-corp'
    subscriptionTags: {
      owner: 'claims-product-owner'
      costCenter: 'CC-1042'
      environment: 'prod'
      workload: 'claims'
      dataClassification: 'confidential'
    }
    roleAssignmentEnabled: true
    roleAssignments: [
      {
        principalId: claimsReadersGroupId
        definition: 'Reader'
        relativeScope: ''
        principalType: 'Group'
      }
    ]
    budgetName: 'budget-claims-prod'
    budgetAmount: budgetFromRequest
    budgetThresholds: [ 80, 100 ]
  }
}

param billingScope string
param claimsReadersGroupId string
param budgetFromRequest int
```

Fije la versión del módulo que su equipo de plataforma haya probado y actualícela de forma deliberada. Observe lo que el ejemplo no hace: ninguna persona recibe acceso de escritura permanente. El rol Contributor del equipo de carga de trabajo se configura como una asignación apta (eligible) mediante PIM para grupos, como describe el capítulo cinco, porque el acceso elevado a una suscripción nueva nunca debe ser permanente de forma predeterminada. Crear suscripciones mediante programación también requiere el rol de facturación adecuado en su Enterprise Agreement, Microsoft Customer Agreement o acuerdo de partner; compruebe esos requisitos previos antes de la primera ejecución.

Los nombres y las etiquetas son parte del contrato

Un nombre le dice a una persona qué es un recurso. Una etiqueta se lo dice a una máquina. Ambos necesitan un estándar que la plataforma haga cumplir, no que se limite a pedir. Para los nombres, seguimos el patrón del Cloud Adoption Framework: tipo de recurso, carga de trabajo, entorno, región e instancia, por ejemplo *vnet-claims-prod-weu-001*. Algunos tipos de recurso restringen los caracteres: los nombres de cuentas de almacenamiento solo admiten letras minúsculas y números, por lo que el mismo patrón se convierte en *stclaimsprodweu001*. Para las etiquetas, mantenga el conjunto obligatorio pequeño y significativo:

Etiqueta	Significado	Cómo se hace cumplir
owner	El equipo o rol responsable, nunca el nombre de una sola persona	El aprovisionamiento la fija en la suscripción; por directiva, los recursos la heredan
costCenter	Dónde se carga el gasto	Igual: se fija una vez y se hereda por directiva
environment	dev, test, prod o sandbox	La fija el aprovisionamiento, coincide con la suscripción
workload	Nombre corto de la carga de trabajo	La fija el aprovisionamiento, coincide con la suscripción
dataClassification	public, internal, confidential, restricted	Obligatoria en los recursos que contienen datos

Azure Policy tiene definiciones integradas para ambas partes. *Inherit a tag from the subscription if missing* usa el efecto Modify para copiar una etiqueta de la suscripción a los recursos, y las tareas de corrección pueden actualizar los recursos existentes. *Require a tag on resources* usa Deny para las etiquetas que solo puede conocer el equipo que realiza la implementación. El capítulo seis explica cómo se comportan esos efectos, y el apéndice contiene un diccionario de etiquetas completo.

> **No haga depender decisiones de seguridad de las etiquetas.** Microsoft advierte que las personas con derechos elevados en una suscripción pueden cambiar las etiquetas. Las etiquetas son excelentes para atribuir costos e identificar responsables; las barreras de protección de seguridad deben estar en el ámbito del grupo de administración, donde los equipos de carga de trabajo no pueden alterarlas.

> *Una suscripción que llega gobernada se mantiene gobernada. Una que llega vacía se convierte en la nube privada de alguien.*

LISTA DE VERIFICACIÓN DEL CONTRATO

- Cada carga de trabajo tiene suscripciones separadas de desarrollo, pruebas y producción en el mismo grupo de arquetipo, o una excepción por escrito.
- Las suscripciones nuevas provienen solo del pipeline de aprovisionamiento, con los datos de la solicitud guardados en la herramienta de administración de servicios.
- Cada suscripción aprovisionada tiene las etiquetas de responsable, centro de costo, entorno y carga de trabajo, y un presupuesto con alertas.
- Ninguna persona recibe acceso de escritura permanente en una suscripción aprovisionada; los roles elevados se asignan como aptos mediante PIM.
- Los nombres siguen un único patrón documentado, y las reglas de etiquetas se hacen cumplir mediante directivas, no mediante revisiones.

Véalo en vivo: el mapa de la zona de aterrizaje en hub.jcardena.com/azure/governance-landing-zone.html

PARTE III · ACCESO Y REGLAS

CAPÍTULO CINCO

Roles: quién puede hacer qué, y durante cuánto tiempo

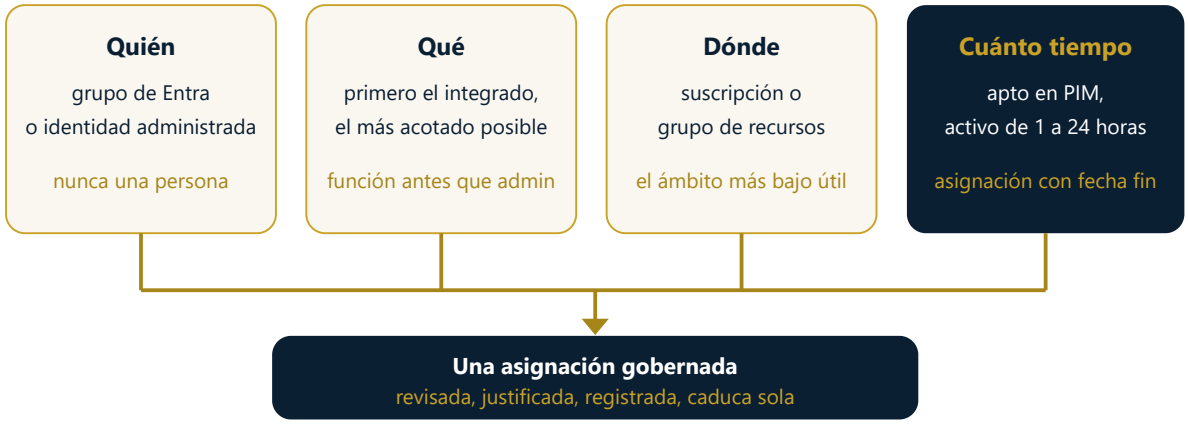


En la mayoría de los entornos, el acceso tiene fecha de inicio y no tiene fecha de finalización. Alguien necesitó arreglar algo una vez, recibió Owner y todavía lo conserva. La solución es fácil de enunciar: conceda el acceso a grupos, no a personas; otorgue el rol con menos permisos en el ámbito más bajo posible; y haga que todo rol con privilegios elevados sea temporal: que se active solo cuando se necesite y caduque por sí solo.

El control de acceso basado en roles de Azure (Azure RBAC) responde a la pregunta "quién puede hacer qué, y dónde". Cada asignación de roles tiene tres partes: una entidad de seguridad (un usuario, un grupo, una entidad de servicio o una identidad administrada), una definición de rol (un conjunto de acciones permitidas) y un ámbito (grupo de administración, suscripción, grupo de recursos o recurso). Las asignaciones en un ámbito primario las heredan todos los ámbitos secundarios. GDCD agrega una cuarta parte que RBAC por sí solo deja abierta: **durante cuánto tiempo**.

FIGURA 5.1

Las cuatro preguntas de toda asignación de roles



RBAC responde a tres preguntas. El contrato necesita cuatro. Privileged Identity Management aporta la cuarta: un acceso apto (eligible), que se activa por un tiempo acotado y queda registrado con un motivo.

Primero los roles integrados, y sepa cuáles son privilegiados

Azure tiene cientos de roles integrados. Microsoft los agrupa en dos tipos. Los roles de función de trabajo administran tipos de recursos concretos, por ejemplo Virtual Machine Contributor o Storage Blob Data Reader. Los roles de administrador con privilegios otorgan una administración amplia o la capacidad de conceder acceso a otros. Microsoft considera privilegiados los siguientes:

Rol	Por qué es privilegiado	Configuración predeterminada gobernada
Owner	Administración completa de todos los recursos, y puede asignar roles	Solo apto, grupo pequeño de plataforma, aprobación obligatoria en producción
Contributor	Administración completa de todos los recursos, no puede asignar roles	Apto para los equipos de carga de trabajo en sus propias suscripciones
User Access Administrator	Administra el acceso, puede concederse a sí mismo o a otros el rol Owner	Apto, solo para el equipo de identidad de la plataforma
Role Based Access Control Administrator	Administra el acceso, puede conceder Owner salvo que se restrinja	Usar con una condición que limite qué roles puede asignar
Reservations Administrator	Administra todas las reservas del inquilino	Solo el equipo de FinOps, apto

Prefiera un rol de función de trabajo siempre que exista. Un equipo que necesita leer blobs recibe Storage Blob Data Reader, no Contributor y desde luego no Owner. Cuando deba delegar la capacidad de asignar roles, Microsoft recomienda agregar una condición a la asignación de Role Based Access Control Administrator para que el delegado solo pueda conceder los roles concretos que usted permita, por ejemplo solo roles de lector de datos, y nunca Owner. Microsoft también recomienda un máximo de tres propietarios por suscripción, una comprobación sobre la que informa Microsoft Defender for Cloud. Cree roles personalizados solo cuando ningún rol integrado encaje, enumere sus acciones de forma explícita sin caracteres comodín y haga referencia a los roles por su identificador en la automatización, porque los nombres pueden cambiar.

Grupos, no personas

Asigne los roles a grupos de Microsoft Entra, nunca directamente a usuarios. Así se mantiene bajo el número de asignaciones, lo cual importa porque Azure limita las asignaciones de roles por suscripción y por grupo de administración. Más importante aún, traslada la pregunta "¿debe esta persona tener acceso?" a la pertenencia al grupo, donde los procesos de altas, cambios y bajas y las revisiones de acceso pueden responderla. Un patrón de nombres ayuda a todos a leer el modelo, por ejemplo *grp-claims-prod-contributor*: carga de trabajo, entorno, rol.

Justo a tiempo con Privileged Identity Management

Microsoft Entra Privileged Identity Management (PIM) convierte el acceso permanente en acceso apto. Un miembro apto tiene el derecho de activar un rol, no el rol en sí. Para usarlo, lo activa por un tiempo acotado, y PIM puede exigir, por rol y por ámbito:

- Una duración de activación de entre 1 y 24 horas, fijada como máximo por el administrador.
- Autenticación multifactor, o un contexto de autenticación de acceso condicional que exija una intensidad de autenticación específica o un dispositivo conforme.
- Una justificación de negocio y, opcionalmente, un número de ticket.
- La aprobación de aprobadores designados. No hay aprobadores predeterminados, y Microsoft recomienda al menos dos. Decide el primer aprobador que responde, por lo que dos aprobadores aportan disponibilidad, no doble control; cuando un cambio requiera a dos personas, hágalo cumplir en el pipeline o en el proceso de cambios.
- Una fecha de finalización en la propia asignación apta, de modo que incluso la condición de apto caduca y debe renovarse.

La configuración de PIM se define por rol y por recurso, y la configuración de una suscripción no la heredan los grupos de recursos que están por debajo. Configúrela de forma deliberada en cada ámbito donde conceda acceso, desde código cuando sea posible. PIM para grupos permite que la pertenencia a un grupo privilegiado sea apta, y así es como una suscripción aprovisionada puede conceder Contributor a un equipo de carga de trabajo sin concederlo de forma permanente. PIM requiere licencias de Microsoft Entra ID P2 o Microsoft Entra ID Governance para los usuarios con asignaciones aptas y para los aprobadores; confirme la cobertura antes de diseñar en torno a esta función.

FIGURA 5.2

Una matriz de roles por perfil y entorno (resumen; la versión completa está en el apéndice)

Perfil	Desarrollo	Pruebas	Producción
Desarrollador de la carga de trabajo	Contributor, apto, sin aprobación	Reader permanente; Contributor apto	Reader permanente; sin escritura
Líder de la carga de trabajo	Contributor, apto	Contributor, apto	Contributor, apto, con aprobación obligatoria
Ingeniero de plataforma	Owner apto en el grupo de administración Landing zones; roles aptos separados en el grupo de administración Platform o en sus suscripciones, con privilegio mínimo; aprobación obligatoria, con al menos dos aprobadores configurados		
Pipeline de implementación	Contributor en su propia suscripción	Contributor en su propia suscripción	Contributor en su propia suscripción, con identidad separada
Operaciones de seguridad	Security Reader permanente; Security Admin apto		

El acceso de escritura en producción nunca es permanente para una persona. En producción, las personas leen; los pipelines escriben. Las personas escriben solo mediante una activación aprobada y limitada en el tiempo.

Identidades de carga de trabajo: sin claves compartidas

Los pipelines y las aplicaciones también necesitan identidades, y no pueden tener roles aptos en PIM, porque no pueden completar una activación. Sus asignaciones de roles siempre están activas, y por eso el ámbito debe ser reducido y la credencial no debe filtrarse. El contrato para las identidades de carga de trabajo:

- **Identidades administradas** para los recursos de Azure que se comunican con otros servicios de Azure. No existe ningún secreto que robar.
- **Federación de identidades de carga de trabajo** para los pipelines de GitHub Actions o Azure DevOps. El pipeline intercambia su propio token por un token de Entra; no se almacena ningún secreto de cliente.
- **Una identidad por pipeline y por entorno.** La identidad del pipeline de producción no puede implementar en desarrollo, ni a la inversa.
- **Un inventario con responsables.** Cada entidad de servicio e identidad administrada tiene un responsable identificado y un propósito; todo secreto o certificado que siga existiendo tiene una fecha de caducidad supervisada; las identidades sin responsable o sin inicios de sesión recientes se revisan y se eliminan.
- **Autenticación de Entra ID antes que claves.** Cuando un servicio admita la autenticación de Entra ID, desactive la autenticación basada en claves o local, y hágalo cumplir con una directiva (capítulo seis).

Revisiones y evidencia

El acceso que no se revisa acaba volviendo a ser permanente. Ejecute revisiones de acceso sobre los grupos privilegiados y sobre las asignaciones aptas, como mínimo trimestralmente para producción, y deje que los responsables confirmen o retiren el acceso. Después compruebe el resultado de forma independiente. Azure Resource Graph expone las asignaciones de roles, de modo que una consulta programada puede encontrar lo que el contrato prohíbe, por ejemplo un rol privilegiado asignado directamente a un usuario:

```
authorizationresources
| where type =~ "microsoft.authorization/roleassignments"
| extend roleDefinitionId = tostring(properties.roleDefinitionId),
         principalType = tostring(properties.principalType),
         scope = tostring(properties.scope)
| extend roleId = tostring(split(roleDefinitionId, "/")[-1])
| where roleId in~ (
    "8e3af657-a8ff-443c-a75c-2fe8c4bcb635",   // Owner
    "b24988ac-6180-42a0-ab88-20f7382dd24c",   // Contributor
    "18d7d88d-d35e-4fb5-a5c3-7773c20a72d9",   // User Access Administrator
    "f58310d9-a9f6-439a-9e8d-f62e7b41a168")   // Role Based Access Control Administrator
| where principalType == "User"
| project scope, roleDefinitionId, principalId = tostring(properties.principalId)
```

Las asignaciones activas aparecen en esta tabla, incluidos los roles de PIM activados mientras estén activos. Un resultado vacío es el resultado de un control, no una prueba por sí solo: consérvelo junto con la consulta, el ámbito y la marca de tiempo, al lado de las

revisiones de pertenencia a grupos y de PIM que cubren el acceso concedido mediante grupos. Un resultado no vacío es un hallazgo con un ámbito y una entidad de seguridad, listo para que el responsable lo corrija.

Otros dos colectivos necesitan la misma disciplina. Los invitados de organizaciones asociadas deben llegar mediante paquetes de acceso de administración de derechos en Microsoft Entra ID Governance, que incluyen un aprobador y una fecha de caducidad, y seguir cubiertos por revisiones de acceso periódicas. Las entidades de servicio con roles privilegiados también pueden incluirse en las revisiones de acceso de PIM, lo que requiere licencias de Workload Identities Premium además de P2 o ID Governance, para que una cuenta de automatización olvidada se detecte mediante el mismo proceso que una persona olvidada.

LA LIMPIEZA DEL ACCESO PERMANENTE

En una primera revisión típica, la mayoría de las asignaciones directas a usuarios resultan ser restos de proyectos ya terminados. El equipo de plataforma no las elimina de una sola vez. Publica la lista, convierte las que todavía se necesitan en asignaciones aptas basadas en grupos, da a los responsables un plazo fijo y luego elimina el resto. La consulta de Resource Graph anterior se convierte en el control que mantiene el número en cero.

> *El acceso debe comportarse como la llave de un hotel, no como la de una casa: se entrega para una estancia, se registra en la puerta y deja de funcionar al salir.*

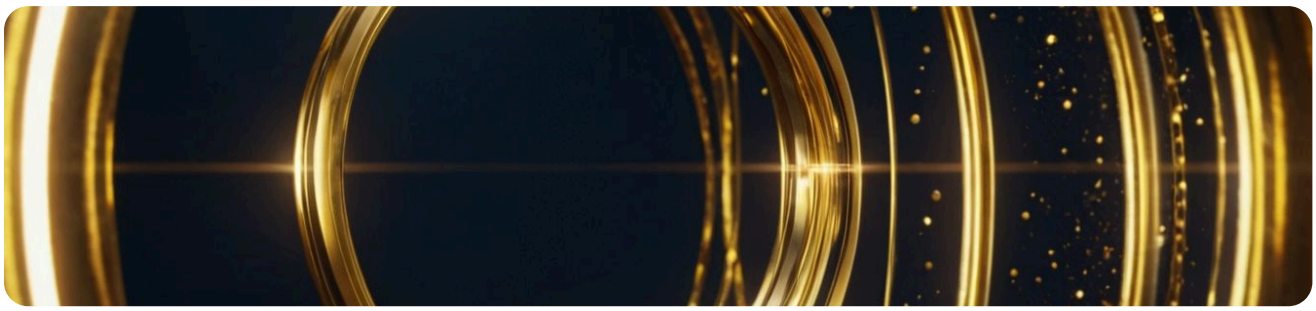
LISTA DE VERIFICACIÓN DEL CONTRATO

- Todas las asignaciones de roles para personas se hacen a grupos, no a usuarios.
- Ninguna persona tiene Owner, Contributor o User Access Administrator permanente en producción.
- PIM exige MFA y justificación para cada rol privilegiado, y aprobación para producción.
- Ninguna suscripción tiene más de tres propietarios.
- Los pipelines usan federación de identidades de carga de trabajo o identidades administradas, una identidad por entorno, sin secretos almacenados.
- Las revisiones de acceso se ejecutan al menos trimestralmente sobre los grupos privilegiados, y una consulta programada informa de las asignaciones directas a usuarios.

Véalo en vivo: el mapa de roles en hub.jcardena.com/azure/governance-roles.html

CAPÍTULO SEIS

La directiva es el contrato que se ejecuta



Un estándar escrito en un documento se comprueba cuando alguien se acuerda de comprobarlo. Un estándar escrito como directiva de Azure Policy lo comprueba la propia plataforma en cada creación y en cada actualización, y su cumplimiento se notifica todos los días. Esa es la diferencia entre un deseo y un contrato. En la directiva, las garantías del capítulo uno dejan de ser promesas y empiezan a hacerse cumplir.

Azure Policy evalúa los recursos según reglas, e informa de lo que encuentra o actúa en consecuencia. Cada definición de directiva tiene una regla y un efecto. Las definiciones se agrupan en iniciativas, también llamadas conjuntos de directivas, y ambas se asignan a un ámbito: un grupo de administración, una suscripción o un grupo de recursos. Las asignaciones se heredan hacia abajo por el árbol del capítulo tres, de modo que una sola asignación en el grupo Landing zones gobierna todas las suscripciones de carga de trabajo que están por debajo.

FIGURA 6.1

El ciclo de vida de la directiva: de la regla a la evidencia



La asignación es donde se firma el contrato. La definición dice qué se comprueba. La asignación dice dónde, con qué parámetros, en qué modo de aplicación y con qué identidad, si tiene que corregir algo.

Los efectos, en palabras sencillas

Azure Policy admite estos efectos: addToNetworkGroup, append, audit, auditIfNotExists, deny, denyAction, deployIfNotExists, disabled, manual, modify y mutate. Cinco de ellos sostienen la mayor parte de la gobernanza empresarial, y cada uno es un tipo distinto de cláusula contractual.

Efecto	Qué hace	Cláusula del contrato
Audit	Permite la solicitud y marca el recurso como no conforme. Juzga el recurso por sus propias propiedades.	"Lo sabremos." Observe antes de hacer cumplir.
AuditIfNotExists	Marca un recurso como no conforme cuando falta un recurso relacionado, por ejemplo una máquina virtual sin una extensión obligatoria.	"Sabremos si falta el recurso asociado."
Modify	Agrega, actualiza o quita propiedades o etiquetas al crear o actualizar, y puede corregir recursos existentes.	"Lo corregiremos por usted." Típico para etiquetas.
DeployIfNotExists	Implementa un recurso relacionado cuando falta, por ejemplo una configuración de diagnóstico que envía los registros al área de trabajo central de Log Analytics.	"Agregaremos lo que sea obligatorio."
Deny	Rechaza la solicitud de creación o actualización antes de que llegue al proveedor de recursos.	"Esto no va a ocurrir."

Dos detalles importan en la práctica. Modify y DeployIfNotExists cambian recursos, por lo que sus asignaciones necesitan una identidad administrada con los roles adecuados para hacer el trabajo, y los recursos existentes se corrigen mediante tareas de corrección. Y cuando varias asignaciones se aplican al mismo recurso, cada una se evalúa de forma independiente y el resultado neto es acumulativo y prevalece lo más restrictivo: si cualquier asignación deniega, la solicitud se deniega.

Un conjunto inicial que se deriva de los resultados

Cada directiva del conjunto debe poder rastrearse hasta una garantía. Los aceleradores de zonas de aterrizaje asignan una línea base razonable, y nosotros agregamos las reglas que exigen nuestros resultados. Un conjunto inicial típico, por ámbito:

Garantía	Directiva (integrada cuando existe)	Efecto	Ámbito
Los recursos se implementan solo en regiones aprobadas	Allowed locations	Deny	Landing zones
Cada recurso tiene un responsable y un centro de costo	Inherit a tag from the subscription if missing	Modify	Raíz intermedia
Ningún punto de conexión PaaS público para cargas de trabajo corporativas	Public network access should be disabled for PaaS services (iniciativa de zona de aterrizaje)	Deny	Corp
Cada suscripción envía sus registros a un solo lugar	Configuración de diagnóstico hacia el área de trabajo central de Log Analytics	DeployIfNotExists	Raíz intermedia
La línea base de seguridad se mide	Microsoft cloud security benchmark	Audit, AuditIfNotExists	Raíz intermedia

El conjunto inicial completo, con los efectos para sandbox y para las zonas de aterrizaje, está en el apéndice. Las directivas de red y de seguridad se tratan junto con sus capas en los capítulos siete y ocho.

Observe lo que promete la directiva Allowed locations y lo que no. Controla la ubicación de los recursos que cubre. No demuestra, por sí sola, por dónde viajan los datos: los servicios globales, la replicación geográfica, el almacenamiento de copias de seguridad y los procesos de soporte tienen cada uno su propia configuración. Una garantía de residencia de datos necesita también esa configuración de los servicios, escrita en el mismo contrato.

Primero auditar, luego denegar, y la trampa de "auditar en desarrollo"

Una regla práctica habitual es "auditar en desarrollo, denegar en producción". Nosotros usamos otra, porque la guía de zonas de aterrizaje de Microsoft desaconseja dar barreras de protección distintas a desarrollo, pruebas y producción: los equipos construyen con las reglas más flexibles y luego fallan en el último paso de promoción. Nuestra regla es **auditar primero, denegar cuando ya no queden incumplimientos y mantener las mismas barreras de protección en todos los entornos**. Auditar y denegar son etapas en el tiempo, no diferencias entre entornos. Sandbox es el único lugar con un conjunto deliberadamente más flexible.

Para aplicar esta regla con coherencia, hay que hacer una distinción. Las barreras de protección son las reglas sobre ubicación, exposición de red, identidad y configuración de seguridad, y son idénticas en desarrollo, pruebas y producción. Los parámetros de costo y escala, como la lista de SKU permitidas, el apagado automático o el nivel de detalle de los registros de los recursos, pueden variar según el entorno (capítulo diez); establézcalos como parámetros en el ámbito de la suscripción durante el aprovisionamiento. Producción puede agregar obligaciones, como la copia de seguridad. Ningún entorno elimina una barrera de protección.

Azure Policy le ofrece las herramientas para escalonar ese despliegue con seguridad:

- **Modo de aplicación.** Una asignación con enforcementMode establecido en DoNotEnforce evalúa el cumplimiento e informa de él sin aplicar el efecto, de modo que puede ver el impacto de un Deny antes de que bloquee a nadie.
- **Selectores de recursos.** Limite primero una asignación nueva a ciertas regiones o tipos de recurso, y luego amplíela por pasos.
- **Invalidaciones.** Cambie el efecto de determinadas definiciones dentro de una iniciativa, por ejemplo de audit a deny, sin editar las definiciones.
- **Mensajes de incumplimiento.** Un Deny debe decirle al ingeniero por qué, y dónde consultar. Un mensaje personalizado es parte del contrato.

```
targetScope = 'managementGroup'

resource allowedLocations 'Microsoft.Authorization/policyAssignments@2024-04-01' = {
  name: 'allowed-locations'
  properties: {
    displayName: 'Resources only in approved regions'
    policyDefinitionId: '/providers/Microsoft.Authorization/policyDefinitions/e56962a6-
4747-49cd-b67b-bf8b01975c4c'
    enforcementMode: 'DoNotEnforce'   // fase 1: solo informar; cambiar a 'Default'
cuando no haya incumplimientos
    parameters: {
      listOfAllowedLocations: { value: [ 'westeurope', 'northeurope' ] }
    }
    nonComplianceMessages: [
      { message: 'Region not approved. See the platform guide or contact the platform
team.' }
    ]
  }
}
```

Cuando un entorno realmente necesite una obligación adicional, como una copia de seguridad solo en producción, Microsoft sugiere asignarla en el ámbito de la suscripción durante el aprovisionamiento, o auditarla en el ámbito del grupo de administración y dejar que el equipo de carga de trabajo la implemente. Mantenga las barreras de protección de seguridad en el ámbito del grupo de administración. Las asignaciones en el ámbito de la suscripción las pueden modificar las personas con derechos elevados en esa suscripción, y esa es también la razón por la que los permisos para escribir asignaciones, definiciones y exenciones de directivas nunca deben ser permanentes; gestiónelos mediante PIM.

Exenciones con fecha de caducidad

Todo entorno real tiene excepciones. Un contrato sin una forma de gestionarlas termina siendo eludido. Las exenciones de Azure Policy son la vía autorizada, e incluyen exactamente los campos que necesita un contrato de gobernanza: qué asignación, qué definiciones dentro de ella, una categoría, metadatos sobre quién la solicitó y quién la aprobó, y una fecha de caducidad.

```
{
  "properties": {
    "displayName": "Claims legacy API: public endpoint until migration",
    "policyAssignmentId": "/providers/Microsoft.Management/managementGroups/org-
corp/providers/Microsoft.Authorization/policyAssignments/deny-public-endpoints",
    "exemptionCategory": "Waiver",
    "expiresOn": "2027-03-31T23:59:00.0000000Z",
    "metadata": {
      "requestedBy": "claims workload team",
      "approvedBy": "platform security lead",
      "ticketRef": "CHG-0000"
    }
  }
}
```

Hay dos categorías. **Waiver** significa que el incumplimiento se acepta temporalmente. **Mitigated** significa que la intención de la directiva se cumple de otra manera. Cuando se alcanza la fecha de expiresOn, Azure no elimina la exención; conserva el objeto como constancia y simplemente deja de aplicarla, de modo que el recurso vuelve a ser no conforme y, con Deny, su siguiente actualización se bloquea. Crear una exención requiere un permiso propio sobre la asignación de destino, además del acceso de escritura normal, y roles integrados como Resource Policy Contributor y Security Admin pueden administrarlas.

NUESTRO CONTRATO DE EXENCIONES

- Cada exención tiene una fecha de caducidad. Fijamos un máximo de un trimestre para las de tipo Waiver, renovable una vez con una nueva aprobación.
- Las exenciones Waiver necesitan un plan de migración. Las exenciones Mitigated identifican el control compensatorio, su responsable y la evidencia de que funciona, por ejemplo un firewall de aplicaciones web delante de un punto de conexión público más una alerta sobre sus registros.
- Todas las exenciones y sus controles compensatorios están en un único registro, generado a partir de los metadatos de las exenciones, que un auditor puede consultar sin tener que pedirlo.
- El solicitante, el aprobador y el ticket constan en los metadatos, no en la bandeja de entrada de alguien.
- Un informe mensual enumera las exenciones que vencen en los próximos 30 días y las vencidas que siguen registradas.

Exento no es lo mismo que excluido. Una exención mantiene visible el recurso con un estado de cumplimiento Exempt, y Azure registra cuál sería su estado sin la exención. Excluir un ámbito con notScopes lo saca por completo de la evaluación. Use exenciones para las excepciones y reserve notScopes para razones estructurales que pueda defender.

CUANDO EL CONTRATO DECIDE

Un equipo de carga de trabajo pide un punto de conexión público en una cuenta de almacenamiento de producción porque una integración con un socio lo necesita esta semana. Con un estándar basado en documentos, la respuesta depende de a quién se le pregunte. Con la directiva, decide el efecto Deny asignado en Corp, y el camino es claro: solicitar una exención Waiver, presentar el plan para pasar a conectividad privada, obtener la aprobación y recibir una exención que vence al final del trimestre. El ingeniero sigue adelante en un día. La excepción es visible, tiene responsable y es temporal.

El modelo propone. El contrato decide. Aquí el modelo es la solicitud de un ingeniero, y la exención, con su fecha, es la forma en que el contrato dice "sí, por ahora".

LISTA DE VERIFICACIÓN DEL CONTRATO

- Cada directiva asignada se remonta a una garantía escrita y a un responsable.
- Las barreras de protección se asignan en el ámbito del grupo de administración y son las mismas para desarrollo, pruebas y producción; solo Sandbox es distinto.
- Las nuevas asignaciones Deny se ejecutan primero en DoNotEnforce o en auditoría, con una fecha fijada para pasar a la aplicación (Deny activo).
- Las asignaciones Modify y DeployIfNotExists tienen una identidad administrada con roles de privilegio mínimo, y la corrección se ejecuta sobre los recursos existentes.
- Cada exención tiene una categoría, metadatos del aprobador y una fecha de caducidad, y las próximas a vencer se incluyen en un informe mensual.
- Los permisos para cambiar asignaciones, definiciones y exenciones de directivas se obtienen mediante asignaciones aptas (eligible) en PIM, nunca como acceso permanente.

Véalo en vivo: el mapa de directivas en hub.jcardena.com/azure/governance-policy.html

PARTE IV · CAPAS DE GARANTÍA

CAPÍTULO SIETE

Red: privada de forma predeterminada



Lo esencial, en palabras sencillas: en un entorno gobernado, ningún servicio de datos es accesible desde internet a menos que alguien haya dejado por escrito por qué, y la plataforma comprueba esa promesa cada vez que se crea un recurso. Lo privado es la opción predeterminada. Lo público es la excepción, y una excepción tiene un responsable, un motivo y una fecha de finalización.

Las partes II y III dieron al entorno su estructura y sus reglas. El capítulo tres ubicó un grupo de administración Connectivity bajo Platform. El capítulo cuatro dio a cada carga de trabajo su propia suscripción por entorno. El capítulo seis hizo de la directiva el contrato que se ejecuta. En este capítulo, esas piezas llegan a la red propiamente dicha. La red es la primera capa de garantía porque decide qué puede llegar siquiera a un recurso antes de que la identidad, el cifrado o la supervisión tengan ocasión de ayudar.

La garantía que escribimos es breve: **los servicios de datos de cada entorno de carga de trabajo aceptan tráfico solo por rutas privadas; todo el tráfico de salida abandona la red por un punto que inspeccionamos y registramos; la resolución de nombres funciona igual desde cada spoke y desde la oficina.** O se cumple cada línea, o la garantía es solo un deseo.

Elija primero la forma: hub-and-spoke o Virtual WAN

El Microsoft Cloud Adoption Framework describe dos topologías de red para una zona de aterrizaje. Ambas colocan los servicios de red compartidos en un lugar central y conectan a él las redes de las cargas de trabajo. Se diferencian en quién gestiona el enrutamiento.

- **Topología hub-and-spoke (red en estrella) tradicional.** Usted construye la red virtual del hub, empareja cada spoke con ella y administra el enrutamiento y la seguridad. El marco la sugiere cuando implementa en una o pocas regiones, tiene un

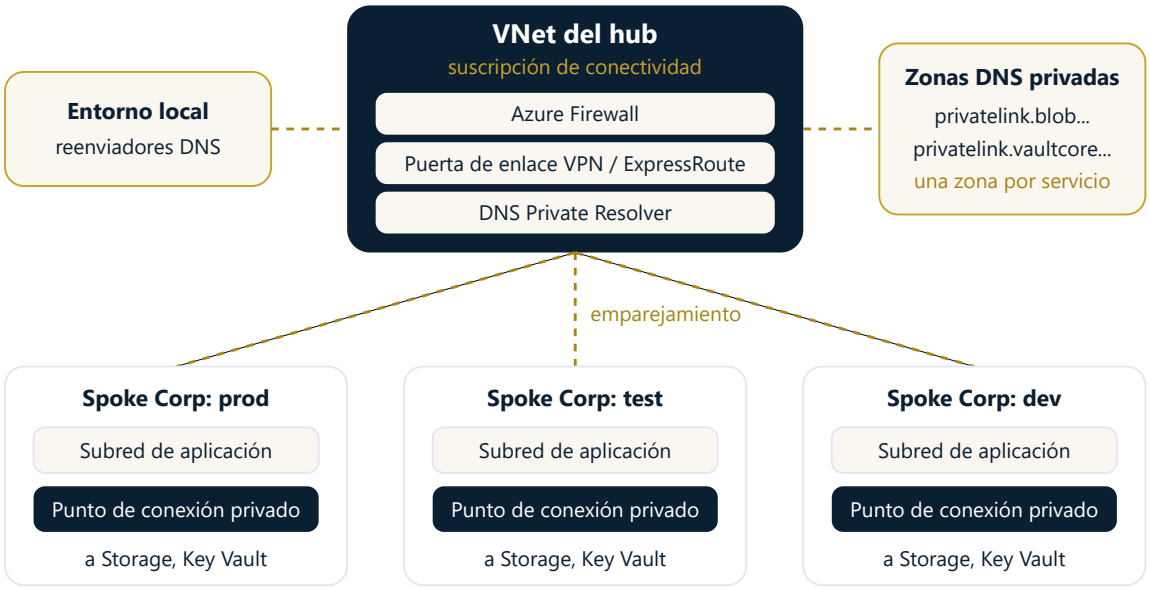
número moderado de sucursales y quiere un control completo y manual del enrutamiento.

- **Azure Virtual WAN.** Un servicio administrado por Microsoft gestiona los hubs y buena parte del enrutamiento. El marco lo sugiere para la conectividad global entre muchas regiones y muchas ubicaciones locales, para grandes redes de sucursales SD-WAN, o cuando necesita enrutamiento transitivo entre VPN y ExpressRoute.

Elija según esos criterios, no por costumbre. Hub-and-spoke suele ser el inicio más sencillo en una o pocas regiones, porque es más fácil de entender y de explicar a un auditor; Virtual WAN se gana su lugar cuando el requisito es un enrutamiento global y administrado. El contrato es el mismo en ambos casos. El patrón sobrevive a la elección del producto: un hub por región, propiedad del equipo de plataforma, ubicado en la suscripción de conectividad; spokes propiedad de los equipos de carga de trabajo, ubicados en sus propias suscripciones de zona de aterrizaje; ningún spoke se comunica con otro spoke salvo a través del hub.

FIGURA 7.1

Hub-and-spoke con puntos de conexión privados y DNS central



El hub es dueño de las puertas compartidas; los spokes son dueños de sus cargas de trabajo. Cada spoke llega a los servicios de datos a través de un punto de conexión privado en su propia subred. Los registros DNS de esos puntos de conexión residen en zonas DNS privadas centrales que solo administra el equipo de plataforma, de modo que cada spoke y la oficina resuelven el mismo nombre a la misma dirección privada.

Puntos de conexión privados: la puerta de los datos

Un punto de conexión privado es una interfaz de red en su red virtual que obtiene una dirección IP privada y se conecta a un servicio de plataforma, como una cuenta de almacenamiento, un almacén de claves o una base de datos. El tráfico hacia ese servicio permanece entonces en rutas privadas. Combínelo con la desactivación del acceso de red público en el propio servicio, y el servicio rechazará las llamadas desde internet, independientemente de lo que se escriba.

Ese último paso es importante. La documentación de Microsoft es explícita en que la resolución DNS y el control de acceso son independientes. El nombre público de un recurso sigue resolviéndose desde cualquier lugar; lo que detiene a un cliente externo es la propia configuración de acceso de red público o el firewall del servicio. Un punto de conexión privado sin esa configuración es una segunda puerta, no una primera puerta cerrada con llave.

Los puntos de conexión privados fallan en silencio en el DNS

Las aplicaciones siguen usando el nombre normal del servicio, por ejemplo el punto de conexión de blobs de una cuenta de almacenamiento. El DNS público de Azure responde con un alias hacia una zona `privatelink`, y su zona DNS privada responde a ese alias con la IP privada. Si falta la zona privada, está vinculada a la red equivocada o está duplicada en un spoke, la aplicación llega al punto de conexión público (y es rechazada) o no logra resolver el nombre en absoluto. El síntoma parece un error de la aplicación. La causa es un contrato roto en la puerta del DNS.

El patrón del Cloud Adoption Framework para hacer esto a escala es el que aplicamos:

1. El equipo de plataforma crea las zonas DNS privadas `privatelink` una sola vez, en la suscripción de conectividad, con los nombres de zona recomendados por Microsoft (por ejemplo `privatelink.blob.core.windows.net` para el almacenamiento de blobs y `privatelink.vaultcore.azure.net` para Key Vault). Use exactamente esos nombres: el alias DNS público de cada servicio apunta a la zona con ese nombre, así que una zona con cualquier otro nombre nunca responde. El registro automático de DNS privado es una función distinta; crea registros solo para máquinas virtuales, no para puntos de conexión privados.
2. Las zonas se vinculan al hub, y todas las redes resuelven a través de un resolvedor en el hub, como Azure DNS Private Resolver. Los servidores DNS locales reenvían de forma condicional las zonas públicas de los servicios al punto de conexión de entrada del resolvedor, por ejemplo `blob.core.windows.net`, no el nombre `privatelink`, tal como especifica la guía de DNS para puntos de conexión privados de Microsoft.

3. Una directiva **Deny** impide que los equipos de carga de trabajo creen sus propias zonas con el prefijo `privatelink`.
4. Una directiva **DeployIfNotExists** vigila los nuevos puntos de conexión privados y agrega un grupo de zonas DNS que escribe el registro en la zona central. Su identidad administrada necesita el rol Private DNS Zone Contributor sobre las zonas. Cuando se elimina el punto de conexión, el registro se elimina con él.

La implementación de referencia de la zona de aterrizaje incluye una iniciativa para esto, titulada "Configure Azure PaaS services to use private DNS zones". Prefiera las definiciones integradas o de referencia frente a las escritas a mano, y manténgalas actualizadas.

La regla de denegación, escrita una sola vez

El capítulo seis fijó la convención: las mismas barreras de protección en desarrollo, pruebas y producción, auditar primero y denegar cuando el entorno ya no tenga incumplimientos. Para la exposición de red, la regla por servicio es breve. Esta rechaza cualquier cuenta de almacenamiento dentro del ámbito que deje activado el acceso de red público:

```
{
  "mode": "All",
  "policyRule": {
    "if": {
      "allOf": [
        { "field": "type", "equals": "Microsoft.Storage/storageAccounts" },
        { "field": "Microsoft.Storage/storageAccounts/publicNetworkAccess",
          "notEquals": "Disabled" }
      ]
    },
    "then": { "effect": "[parameters('effect')]" }
  },
  "parameters": {
    "effect": { "type": "String", "allowedValues": ["Audit", "Deny", "Disabled"],
                "defaultValue": "Audit" }
  }
}
```

La definición se asigna una sola vez, en el grupo de administración Landing zones, con el parámetro de efecto establecido en `Audit`. Cuando la vista de cumplimiento ya no muestra incumplimientos, la misma asignación cambia a `Deny` en una fecha acordada de antemano. Desarrollo, pruebas y producción reciben la misma regla con la misma fuerza, y la fecha del cambio se aplica a todo el ámbito de la zona de aterrizaje a la vez.

Puertas de entrada públicas, segmentación y DDoS

El principio de privado por defecto se aplica a los servicios de datos. Las zonas de aterrizaje Online siguen publicando aplicaciones en internet, y el contrato decide cómo: a través de una única puerta de entrada gobernada, Azure Front Door o Application Gateway con una directiva de Web Application Firewall (WAF), mientras las bases de datos y el almacenamiento que hay detrás permanecen privados. Las directivas integradas *Azure Web Application Firewall should be enabled for Azure Front Door entry-points* y *Web Application Firewall (WAF) should be enabled for Application Gateway* hacen que esa regla se pueda comprobar.

Azure DDoS Protection actúa en las capas de red 3 y 4; el WAF cubre la capa 7. DDoS Network Protection es un plan vinculado a redes virtuales, y un solo plan puede servir a redes virtuales de distintas suscripciones del inquilino; DDoS IP Protection es la alternativa por dirección IP. Sin ninguno de los dos, se sigue aplicando la protección de infraestructura predeterminada. Decida por arquetipo, normalmente Online y cualquier spoke con direcciones IP públicas, registre el costo según el capítulo diez y audite la cobertura con *Virtual networks should be protected by Azure DDoS Protection*.

Dentro de la red, cada subred de carga de trabajo recibe un grupo de seguridad de red y una tabla de rutas que envía el tráfico con destino a internet al firewall del hub. Los grupos de seguridad de aplicaciones permiten que las reglas nombren funciones, como web, aplicación y datos, en lugar de direcciones IP. *Subnets should be associated with a Network Security Group* audita la primera parte; la tabla de rutas la establece el aprovisionamiento junto con el spoke.

Tráfico de salida: una sola salida, y deja registro

El tráfico de entrada privado es la mitad de la garantía. La otra mitad es el tráfico de salida. Los spokes envían el tráfico con destino a internet al firewall del hub mediante una tabla de rutas, y los registros de diagnóstico del firewall llegan al área de trabajo central de Log Analytics que conocerá en el capítulo nueve. Cuando una carga de trabajo necesita un nuevo destino de salida, se trata de un cambio de regla del firewall a través del pipeline del capítulo once, no de una IP pública agregada a toda prisa.

FIGURA 7.2

El contrato de red, escalonado en el tiempo

Regla	Etapa 1: auditoría, días 1 a 60	Etapa 2: aplicación	Se aplica a
Acceso de red público en servicios de datos	Audit	Deny	Desarrollo, pruebas y producción
Zonas DNS privadas creadas en spokes	Audit o DoNotEnforce	Deny	Desarrollo, pruebas y producción
Registros DNS de puntos de conexión privados	DeployIfNotExists hacia las zonas centrales		Desarrollo, pruebas y producción
IP pública en las NIC de máquinas virtuales	Audit	Deny	Desarrollo, pruebas y producción
Tráfico de salida a internet	A través del firewall del hub, con registro central		Cada spoke

Las mismas reglas en todos los entornos, escalonadas en el tiempo. La auditoría es una primera etapa, no una configuración de desarrollo, así que no se construye nada en desarrollo que producción vaya a rechazar. Sandbox conserva su propio conjunto más flexible y no tiene ruta hacia el hub.

UN EJEMPLO COMPUESTO: EL ARREGLO RÁPIDO DEL EQUIPO DE DATOS

Un equipo no puede acceder a su nueva cuenta de almacenamiento desde un agente de compilación y pide acceso público "por una semana". En un entorno sin gobernanza, esa semana se convierte en un año. Aquí la solicitud es una exención de directiva con un responsable, un motivo y una fecha de caducidad (capítulo seis). La causa raíz habitual resulta ser un punto de conexión privado creado sin registro DNS, algo que la directiva DeployIfNotExists ahora corrige por sí sola.

Preste atención a: redes virtuales que usan servidores DNS personalizados que no reenvían al resolvedor del hub; puntos de conexión privados creados con "Integrar con la zona DNS privada" establecido en sí, con lo que se intenta crear una zona en el spoke y la solicitud se rechaza; y servicios que son accesibles de forma privada pero que todavía tienen habilitado el acceso de red público.

La red no es segura porque sea privada. Es segura porque la plataforma se niega a permitir que sea otra cosa, y deja por escrito cada excepción.

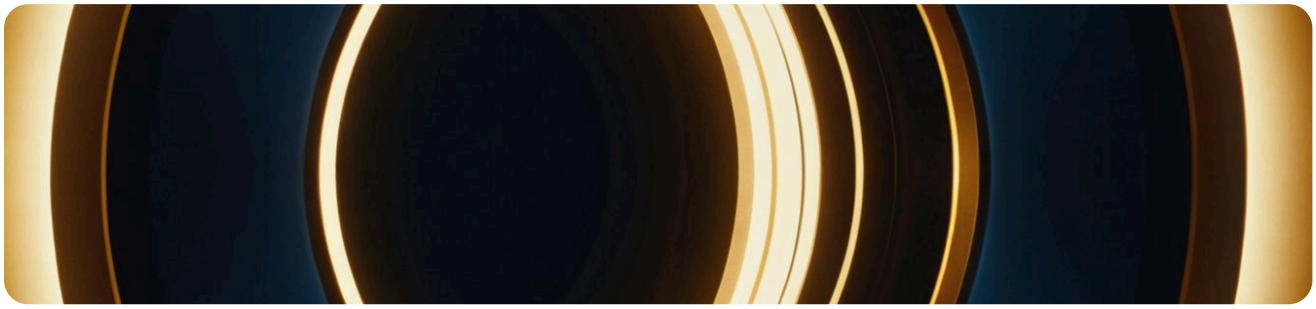
LISTA DE VERIFICACIÓN DEL CONTRATO

- Topología decidida y documentada: hub-and-spoke o Virtual WAN, con el motivo.
- Existen zonas `privatelink` centrales en la suscripción de conectividad, con los nombres recomendados.
- La directiva Deny para el acceso de red público está asignada en el grupo de administración Landing zones, de modo que desarrollo, pruebas y producción reciben la misma regla.
- La directiva DeployIfNotExists crea automáticamente los registros DNS de los puntos de conexión privados.
- Todo el tráfico de salida a internet pasa por el firewall del hub y sus registros llegan al área de trabajo central de Log Analytics.
- Las aplicaciones públicas se publican solo a través de una puerta de entrada con WAF; la protección DDoS se decide por arquetipo; cada subred de carga de trabajo tiene un grupo de seguridad de red, salvo las subredes especiales para las que Azure documenta otra cosa, como GatewaySubnet y AzureFirewallSubnet.

Véalo en vivo: el mapa de la zona de aterrizaje en hub.jcardena.com/azure/governance-landing-zone.html

CAPÍTULO OCHO

Una postura de seguridad que se puede observar



Primero, lo esencial: la seguridad que no se puede ver es seguridad que solo se espera tener. Un entorno gobernado mide su propia postura cada día, muestra esa medida a las personas responsables del riesgo y convierte las correcciones más comunes en reglas, para que el mismo hallazgo no vuelva a aparecer.

El capítulo siete cerró las puertas de red. Este capítulo trata lo que hay detrás de ellas: la postura de cada recurso, los secretos que usan las aplicaciones, las identidades que los usan, los pocos recursos que nunca deben eliminarse por accidente y la promesa de que los datos pueden recuperarse después de un mal día. Cada uno de estos elementos es una garantía. Cada una necesita un mecanismo que la haga cumplir y una evidencia; de lo contrario, no es realmente una garantía.

Defender for Cloud: el medidor de la postura

Microsoft Defender for Cloud evalúa continuamente los recursos de Azure según un estándar de seguridad. Cuando se habilita en una suscripción, se aplica de forma predeterminada el punto de referencia de seguridad en la nube de Microsoft (MCSB), y cada hallazgo se convierte en una recomendación con la lista de los recursos afectados.

Existen dos planes de postura, y la diferencia importa para el presupuesto:

- **Foundational CSPM** es gratuito. Ofrece inventario de recursos, las recomendaciones del MCSB, la puntuación de seguridad, herramientas de corrección y automatización de flujos de trabajo.
- **Defender CSPM** es un plan de pago. Añade el análisis de rutas de ataque, el explorador de seguridad en la nube, la priorización por riesgo, el análisis de vulnerabilidades sin agente, la postura de seguridad de los datos y reglas de gobernanza que asignan los

hallazgos a responsables con fechas de vencimiento.

Los planes independientes de protección de cargas de trabajo (para servidores, almacenamiento, bases de datos, contenedores, Key Vault y otros) añaden detección de amenazas para esos tipos de recursos. El patrón que usamos es sencillo: Foundational CSPM en todas partes desde el primer día; Defender CSPM y los planes de cargas de trabajo en producción y en todo lo que contenga datos regulados, decididos por tipo de recurso y anotados en el modelo de costos del capítulo diez. Los precios y los recursos facturables cambian, así que consulte la página de precios vigente de Defender for Cloud antes de comprometerse.

Puntuación de seguridad: un número, bien leído

La puntuación de seguridad agrupa los hallazgos en un único porcentaje por suscripción, por grupo de administración y para todo el entorno. Un valor más alto significa menos riesgo identificado. Dos detalles permiten interpretarla con rigor:

- Cada control de seguridad gana puntos en proporción a sus recursos en buen estado: su puntuación máxima se reparte entre los recursos que evalúa, y cada recurso en buen estado aporta su parte. Los puntos completos solo llegan cuando se corrigen *todas* sus recomendaciones en *todos* sus recursos, de modo que corregir una recomendación en un recurso que todavía incumple otra del mismo control cambia poco.
- Microsoft ofrece ahora dos modelos. La puntuación de seguridad clásica sigue en Azure Portal. Una Cloud Secure Score basada en el riesgo, que pondera los factores de riesgo y la criticidad de los recursos, está en el portal de Microsoft Defender. Se calculan de forma distinta y producen valores distintos, así que elija una para su cuadro de mando e indique cuál.

Como la puntuación es un dato, se puede consultar. Esta consulta de Azure Resource Graph, tomada del patrón de la documentación de Microsoft, devuelve la puntuación por suscripción para que la revisión operativa del capítulo doce pueda seguir su tendencia:

```
SecurityResources
| where type == 'microsoft.security/securescores'
| extend current = properties.score.current, max = todouble(properties.score.max)
| project subscriptionId, current, max, percentage = ((current / max) * 100)
```

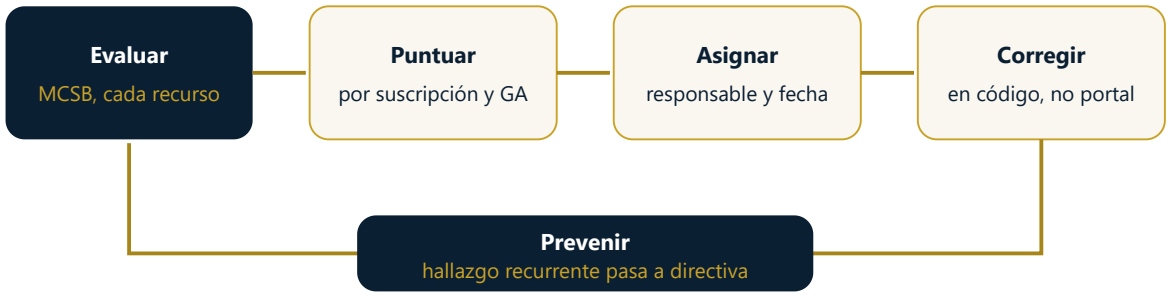
Cumplimiento normativo: la vista del auditor

Los auditores preguntan por estándares, no por puntuaciones. El panel de cumplimiento normativo de Defender for Cloud asigna las evaluaciones a los controles de estándares como ISO/IEC 27001:2022, PCI DSS v4.0.1, NIST SP 800-53 y el Reglamento de Resiliencia

Operativa Digital de la UE (DORA). El MCSB se asigna de forma predeterminada. Para añadir otros estándares se necesita un plan de pago de Defender for Cloud (Defender for Servers Plan 1 y Defender for APIs Plan 1 no sirven) y derechos de Owner o Resource Policy Contributor. En el fondo, cada estándar es una iniciativa de Azure Policy, así que asígnela en el ámbito más alto al que se aplique, normalmente la raíz intermedia. Dos advertencias: los controles que no se pueden evaluar automáticamente aparecen atenuados y siguen necesitando evidencia manual, y un panel en verde es evidencia para una auditoría, no una certificación.

FIGURA 8.1

El ciclo de la postura: medir, asignar, corregir, prevenir



Cada vuelta del ciclo debe dejar un hallazgo menos que corregir a mano.

Una puntuación solo es útil dentro de un ciclo. Defender for Cloud ofrece las acciones Enforce y Deny en muchas recomendaciones; el equipo de plataforma las usa, mediante directivas (capítulo seis), para convertir una corrección repetida en una regla permanente.

Key Vault: secretos con un responsable y un límite

Los secretos, las claves y los certificados se guardan en Azure Key Vault, nunca en el código, en variables del pipeline ni en la configuración de la aplicación. Cuatro prácticas resuelven la mayor parte del problema:

- **Un almacén por aplicación y por entorno.** Es la propia recomendación de Microsoft. Un almacén compartido es un radio de impacto compartido, y las asignaciones de roles sobre secretos individuales se desaconsejan salvo en casos muy concretos.
- **Azure RBAC como modelo de permisos.** Microsoft indica que, a partir de la versión 2026-02-01 de la API de Key Vault, Azure RBAC es el modelo de acceso predeterminado para los almacenes nuevos; las directivas de acceso heredadas se mantienen en los almacenes más antiguos. Use los roles de datos integrados: **Key Vault Secrets User** para una aplicación que lee secretos, **Key Vault Secrets Officer** para el equipo que los

administra, **Key Vault Crypto User** para operaciones criptográficas y **Key Vault Reader** solo para metadatos. Tenga en cuenta que **Key Vault Contributor** administra el propio almacén y no concede acceso a los datos.

- **Ninguna puerta pública.** Acceso de red público deshabilitado, punto de conexión privado como en el capítulo siete y protección de purga activada en los almacenes de producción, de modo que un almacén o secreto eliminado siga siendo recuperable durante su período de retención de eliminación temporal y nadie pueda purgarlo antes de tiempo.
- **Claves bajo su control donde se exija.** Los servicios de Azure cifran los datos en reposo de forma predeterminada con claves administradas por Microsoft. Cuando la clasificación de los datos o un regulador lo exijan, use claves administradas por el cliente guardadas en Key Vault para los servicios que las admiten, con una directiva de rotación en cada clave. Trate la clave como una dependencia de producción: si se deshabilita, se elimina o se revoca su acceso, los servicios que la usan pierden el acceso a sus datos. Mantenga la protección de purga en los almacenes que contienen esas claves, separe a los administradores de claves de los responsables de los datos e incluya la recuperación de claves en el plan de la región de recuperación.

Las aplicaciones acceden al almacén mediante una **identidad administrada**, no con una credencial almacenada. Una identidad asignada por el sistema nace y muere con su recurso; una identidad asignada por el usuario puede compartirse entre unos pocos recursos que realmente forman una sola carga de trabajo. En ambos casos, no hay contraseña que rotar ni nada que se pueda filtrar en un registro.

Bloqueos de recursos: un cinturón de seguridad, no una directiva

Un bloqueo de recursos prevalece sobre los permisos de cualquier usuario en el plano de control. **CanNotDelete** permite cambios pero impide la eliminación. **ReadOnly** impide los cambios y la eliminación. En el portal, esos mismos dos niveles se llaman Eliminar y Solo lectura. Los bloqueos se heredan hacia abajo desde una suscripción o un grupo de recursos, y solo los roles con `Microsoft.Authorization/locks/*`, como Owner y User Access Administrator, pueden crearlos o quitarlos.

Use CanNotDelete en el pequeño conjunto de elementos cuya pérdida detendría el entorno: la red hub, el área de trabajo central de Log Analytics, los almacenes de claves de producción, los almacenes de copias de seguridad y las zonas DNS privadas. Tenga cuidado con ReadOnly. Microsoft documenta efectos secundarios: en una cuenta de almacenamiento impide enumerar las claves; en un grupo de recursos puede impedir que se inicien máquinas virtuales y bloquear el escalado de App Service. Además, los bloqueos solo se aplican al

plano de control. Eliminar un blob, un secreto o las filas de una base de datos sigue funcionando con cualquier bloqueo, así que proteja los datos con eliminación temporal, control de versiones y copias de seguridad.

```
param location string = resourceGroup().location
param kvName string

resource kv 'Microsoft.KeyVault/vaults@2023-07-01' = {
  name: kvName
  location: location
  properties: {
    tenantId: subscription().tenantId
    sku: { family: 'A', name: 'standard' }
    enableRbacAuthorization: true
    enablePurgeProtection: true
    publicNetworkAccess: 'Disabled'
  }
}

resource kvLock 'Microsoft.Authorization/locks@2016-09-01' = {
  name: 'kv-cannot-delete'
  scope: kv
  properties: {
    level: 'CanNotDelete'
    notes: 'Production secrets vault. Removal needs a change record.'
  }
}
```

La aplicación de revisiones tiene un responsable

Los hallazgos de vulnerabilidades solo se cierran cuando alguien aplica la revisión. Azure Update Manager evalúa e instala actualizaciones para máquinas virtuales de Azure y servidores habilitados para Azure Arc; las directivas integradas activan la evaluación periódica, y las configuraciones de mantenimiento fijan las ventanas de revisión por entorno. La matriz RACI del capítulo doce nombra al responsable: el equipo de la carga de trabajo para sus propias máquinas y el equipo de plataforma para las máquinas de la plataforma.

Copia de seguridad y recuperación: una promesa con números

"Tenemos copias de seguridad" es una afirmación. La garantía es un objetivo de punto de recuperación (cuántos datos se pueden perder) y un objetivo de tiempo de recuperación (cuánto tiempo se puede estar sin servicio) por nivel de carga de trabajo, acordados con el responsable de negocio, más la evidencia de que se probó una restauración. Registramos ambos objetivos como etiquetas en la suscripción de producción, protegemos los almacenes de copias de seguridad con bloqueos y programamos cada trimestre una prueba de

restauración cuyo resultado se revisa en el capítulo doce. Active la eliminación temporal y la inmutabilidad en los almacenes de Recovery Services y de Backup, y para los datos regulados bloquee la configuración de inmutabilidad. Solo la inmutabilidad bloqueada es irreversible, de modo que solo en ese caso un administrador comprometido no podrá desactivarla y borrar los puntos de restauración. Azure Policy tiene definiciones integradas que auditan si las máquinas virtuales están protegidas por Azure Backup y otras que lo configuran; audite en el grupo Landing zones y configure en las suscripciones de producción durante el aprovisionamiento, como permite el capítulo seis para las obligaciones exclusivas de producción.

La copia de seguridad responde a la pérdida de datos. La resiliencia responde a una interrupción, y se decide por nivel de carga de trabajo:

- **Redundancia de zona.** En las regiones con zonas de disponibilidad, elija opciones con redundancia de zona para los datos y el cómputo de producción cuando el servicio las ofrezca, de modo que la pérdida de un centro de datos no sea una interrupción.
- **Una región de recuperación designada.** Decida por nivel si la carga de trabajo se recupera en una segunda región, y cómo: Azure Site Recovery para las máquinas virtuales, replicación geográfica o almacenamiento con redundancia geográfica para los servicios de datos. No todas las regiones tienen una región emparejada, así que designe explícitamente la región de recuperación en lugar de dar por supuesta una.
- **La plataforma también se recupera.** El hub, las zonas DNS, el conjunto de directivas y el pipeline de aprovisionamiento deben poder volver a implementarse desde el código en la región de recuperación. El capítulo once es lo que lo hace posible.
- **Prueba.** Una prueba de conmutación por error por nivel, al menos una vez al año, registrando el tiempo de recuperación medido frente al RTO.

> **UN EJEMPLO COMPUESTO: LA PUNTUACIÓN QUE APENAS SE MOVIÓ**
>
> Un equipo de plataforma corrigió decenas de hallazgos y vio que la puntuación de seguridad apenas se movía. Cada corrección era acertada, pero las correcciones estaban muy dispersas: una recomendación aquí, otra allá, en recursos que seguían incumpliendo otras recomendaciones de los mismos controles. Pocos recursos quedaron completamente en buen estado, así que se sumaron pocos puntos. El equipo pasó a cerrar controles completos en conjuntos completos de recursos, empezando por los de mayor puntuación máxima, y trasladó las correcciones recurrentes a directivas de denegación. A partir de entonces la puntuación subió de forma constante y se mantuvo.

> *La postura no es un proyecto que se termina. Es un medidor que se lee, un ciclo que se ejecuta y una lista de reglas que crece cada vez que el mismo error aparece dos veces.*

LISTA DE VERIFICACIÓN DEL CONTRATO

- Defender for Cloud está activado en todas las suscripciones; Defender CSPM y los planes de cargas de trabajo se deciden por entorno y se registran en el modelo de costos.
- El cuadro de mando indica qué modelo de puntuación de seguridad usa y sigue su tendencia cada mes.
- Cada aplicación tiene su propio almacén por entorno, con Azure RBAC y una identidad administrada.
- Los bloqueos CanNotDelete protegen el hub, los registros centrales, los almacenes de producción, las zonas DNS y los almacenes de copias de seguridad.
- Cada carga de trabajo de producción tiene objetivos de RPO y RTO y una restauración probada y fechada.
- Cada nivel de producción tiene una región de recuperación designada, o una decisión escrita de no tenerla, y una prueba de conmutación por error registrada.

Véalo en vivo: la página de directivas y postura en hub.jcardena.com/azure/governance-policy.html

CAPÍTULO NUEVE

Visibilidad: un solo lugar para verlo todo



En pocas palabras: cada cambio, cada registro de recursos y cada alerta del entorno llegan a un único lugar del que es responsable el equipo de plataforma, y cada alerta que importa llega a una persona designada. Si un evento no se puede encontrar después, a efectos de gobernanza no ocurrió, y tampoco actuó el control que debía detectarlo.

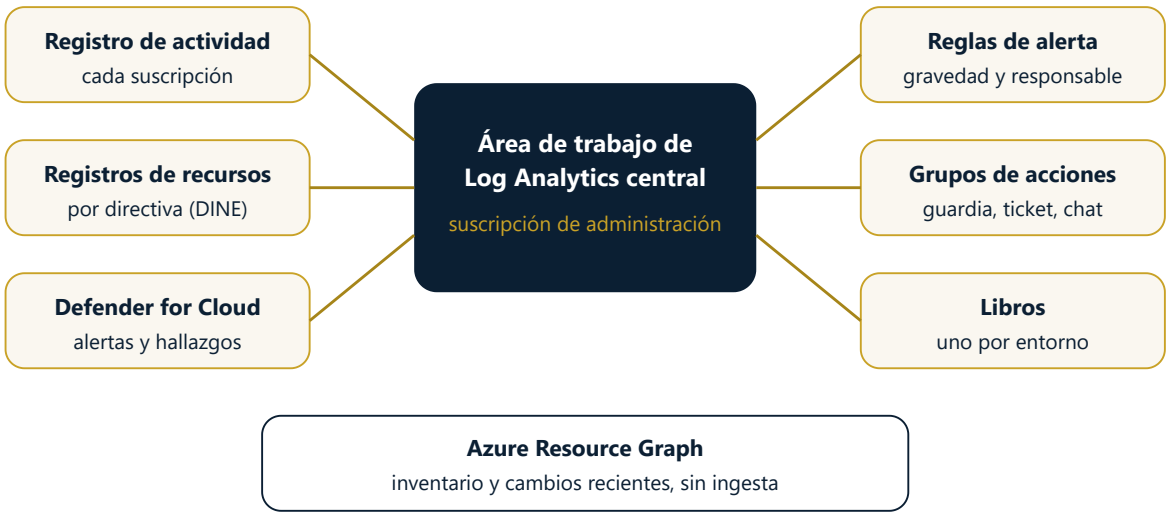
En los capítulos anteriores se escribieron contratos para el inquilino, el árbol, las suscripciones, los roles, las directivas, la red y la postura. Cada contrato tiene una cláusula de evidencia. En este capítulo se reúne esa evidencia. En términos de GDCD, la visibilidad es la capa que convierte las afirmaciones en registros: quién hizo qué, dónde, cuándo y qué decidió el sistema.

Las tres señales y de dónde vienen

- **El registro de actividad** recoge los eventos del plano de control por suscripción: quién creó, cambió o eliminó un recurso, las asignaciones de roles y las decisiones de las directivas. La plataforma lo conserva durante un tiempo limitado, así que lo enviamos al área de trabajo central con una configuración de diagnóstico en el ámbito de la suscripción.
- **Los registros de recursos** los genera cada servicio (accesos a Key Vault, decisiones del firewall, auditorías de bases de datos). Están desactivados hasta que una configuración de diagnóstico los activa, recurso por recurso. Es la carencia que la mayoría de los entornos nunca resuelve a mano.
- **Las métricas y las alertas**, de Azure Monitor y de Defender for Cloud (capítulo ocho), describen el estado y las amenazas casi en tiempo real.

FIGURA 9.1

Señales que entran, decisiones que salen



Un área de trabajo, muchos lectores, con las excepciones que siguen. Los registros fluyen hacia un lugar con responsable; las alertas salen hacia personas designadas. Resource Graph está junto al área de trabajo: responde "qué existe ahora mismo" en todas las suscripciones que usted puede leer, sin recopilar nada.

Primero, un área de trabajo; más, solo con un motivo

La guía de Microsoft sobre el diseño de áreas de trabajo es directa: empiece con una sola área de trabajo de Log Analytics y añada más solo cuando un criterio lo exija. Los principales criterios que enumera son:

- **Inquilinos.** La mayoría de los recursos solo pueden enviar datos a un área de trabajo de su propio inquilino de Microsoft Entra, de modo que un segundo inquilino suele implicar una segunda área de trabajo.
- **Residencia de datos.** Un área de trabajo reside en una sola región; un requisito legal de mantener los datos en una geografía implica tener un área de trabajo allí.
- **Operaciones de seguridad.** Los equipos que usan Microsoft Sentinel suelen mantener un área de trabajo de seguridad dedicada, porque los precios de Sentinel se aplican a todos los datos de un área de trabajo donde está habilitado. Otros combinan ambos usos en una misma área de trabajo para alcanzar un nivel de compromiso. Decídalo una vez y anote el porqué.
- **Retención.** La retención se puede fijar por tabla, así que la única razón de retención para dividir es necesitar retenciones distintas para la misma tabla según el recurso de origen.

En el diseño de zona de aterrizaje de Azure, el área de trabajo está en la suscripción de administración bajo la rama Platform del capítulo tres, su responsable es el equipo de plataforma y está protegida por un bloqueo CanNotDelete (capítulo ocho).

La configuración de diagnóstico es una directiva, no un ticket

Activar los registros de recursos manualmente no es escalable y no cubre el siguiente recurso que se cree. Azure Policy incluye iniciativas integradas que lo hacen para cada tipo de recurso compatible, una por destino y por grupo de categorías de registro. Los dos grupos de categorías son `allLogs` y `audit`. Por ejemplo, la iniciativa **"Enable allLogs category group resource logging for supported resources to Log Analytics"** implementa una configuración de diagnóstico en cada recurso compatible dentro del ámbito.

Tres detalles hacen que funcione. El efecto es **DeployIfNotExists**, así que actúa sobre los recursos nuevos a medida que se crean. Los recursos existentes necesitan una **tarea de corrección**, una por cada directiva de la iniciativa. Y la asignación necesita una **identidad administrada** con un rol que pueda escribir configuraciones de diagnóstico en el ámbito de la asignación. Asigne la iniciativa del grupo de categorías audit una sola vez en la raíz intermedia, de modo que las suscripciones de plataforma queden cubiertas igual que las zonas de aterrizaje, y cada suscripción que crea el proceso de aprovisionamiento (capítulo cuatro) llegue con el registro ya activado. Añada la iniciativa allLogs en las suscripciones de producción durante el aprovisionamiento.

El grupo de categorías es un parámetro de costo, elegido por entorno. Todos los entornos envían `audit` mediante la asignación en la raíz intermedia; producción también envía `allLogs` para los servicios de datos y los recursos relevantes para la seguridad mediante la asignación añadida en el aprovisionamiento, lo que mantiene el costo de ingesta en consonancia con el capítulo diez.

Quién puede leer qué

La visibilidad no debe convertirse en una nueva fuga. De forma predeterminada, un área de trabajo usa el acceso en contexto de recurso: una persona que puede leer un recurso puede leer los registros de ese recurso, sin acceso a toda el área de trabajo. Mantenga ese valor predeterminado para los equipos de cargas de trabajo. Conceda acceso a toda el área de trabajo solo a los equipos de plataforma y de seguridad, y use el control de acceso por tabla cuando una tabla contenga datos que un equipo de carga de trabajo no deba ver.

La evidencia tiene una cláusula de retención

Los registros solo son evidencia mientras se conservan. La retención analítica puede ampliarse hasta dos años por tabla, y la retención total, incluida la retención a largo plazo de bajo costo, hasta 12 años; los datos que superan su período analítico se recuperan con trabajos de búsqueda. Fije la retención por tabla según el período de conservación de registros que exijan sus reguladores y auditores. Cuando la evidencia deba ser a prueba de manipulaciones, exporte además las tablas críticas a una cuenta de almacenamiento con una directiva de inmutabilidad. Si las operaciones de seguridad ejecutan Microsoft Sentinel sobre el área de trabajo, deje por escrito el reparto: el equipo de plataforma es responsable de la ingesta de registros y de la retención; el equipo de seguridad, de las detecciones y los incidentes.

Alertas que llegan a una persona

Una alerta que no llega a nadie es solo una entrada de registro. Cada regla de alerta tiene tres elementos: una gravedad, un grupo de acciones que indica adónde va (equipo de guardia, cola de tickets, canal de chat) y un responsable que decide si sigue siendo útil. Mantenemos la lista corta. Un pequeño conjunto de alertas de plataforma cubre el entorno: una asignación de directiva o de rol cambiada en el ámbito de un grupo de administración, un bloqueo quitado, una eliminación en producción, una configuración de diagnóstico quitada, una alerta de Defender de gravedad alta, y las alertas de Azure Service Health y Resource Health para las regiones y los servicios que usa el entorno, de modo que un incidente de la plataforma o un mantenimiento planificado llegue al equipo de guardia antes de que llamen los usuarios. Los equipos de cargas de trabajo son responsables de sus propias alertas de servicio en sus redes spoke.

Una consulta inicial para la alerta de "eliminaciones en producción", ejecutada sobre el área de trabajo central:

```
AzureActivity
| where CategoryValue == "Administrative" and ActivityStatusValue == "Success"
| where OperationNameValue endswith "/DELETE"
| summarize deletes = count() by Caller, SubscriptionId, bin(TimeGenerated, 1h)
```

Resource Graph: el inventario siempre al día

Azure Resource Graph responde preguntas sobre lo que existe en todas las suscripciones que usted puede leer, con un lenguaje de consulta basado en KQL. No necesita implementar nada y las consultas no tienen costo, aunque están sujetas a límites de frecuencia. También conserva los últimos 14 días de cambios en la configuración de los recursos, lo que a menudo basta para responder "qué cambió desde el martes". Lo usamos para las preguntas que un

área de trabajo de registros responde mal: qué recursos no tienen etiqueta de responsable, qué cuentas de almacenamiento todavía permiten el acceso público, qué suscripciones no tienen presupuesto.

```
resources
| where isnull(tags['owner']) or tostring(tags['owner']) == ''
| summarize untagged = count() by subscriptionId, type
| order by untagged desc
```

Cada entorno tiene un libro de Azure Monitor (workbook) construido sobre estas consultas y sobre el área de trabajo: el cumplimiento de las directivas, la puntuación de seguridad del capítulo ocho, las alertas abiertas, los recursos sin etiquetar y el gasto del capítulo diez. Ese libro es la página que la revisión operativa del capítulo doce abre primero.

UN EJEMPLO COMPUESTO: LAS SEIS HORAS PERDIDAS

En la revisión de un incidente había que saber quién había cambiado una regla del firewall de producción. El registro de actividad mostraba el cambio, pero los registros de recursos del firewall nunca se habían activado, así que nadie podía ver qué tráfico había permitido la regla anterior. La solución no fue una herramienta nueva. Fue asignar la iniciativa allLogs en la raíz intermedia y ejecutar sus tareas de corrección, para que la siguiente revisión tuviera el registro.

Atención a: áreas de trabajo creadas por equipos individuales "solo por ahora", configuraciones de diagnóstico que apuntan a una cuenta de almacenamiento que nadie lee y reglas de alerta cuyo grupo de acciones envía correos a una persona que ya se fue. Resource Graph puede encontrar las tres.

> *La visibilidad es la cláusula de evidencia de todos los demás contratos. Sin ella, la gobernanza es un conjunto de afirmaciones que nadie puede comprobar.*

LISTA DE VERIFICACIÓN DEL CONTRATO

- Un área de trabajo central en la suscripción de administración; cualquier área de trabajo adicional tiene una razón por escrito.
- Los registros de actividad de todas las suscripciones llegan al área de trabajo central, y la retención de las tablas coincide con el período de conservación exigido.
- Hay una iniciativa integrada de configuración de diagnóstico asignada en la raíz intermedia, con las tareas de corrección ejecutadas.
- Cada alerta de plataforma, incluida Service Health, tiene una gravedad, un grupo de acciones y un responsable.
- Un libro por entorno muestra el cumplimiento, la postura, las alertas, los recursos sin etiquetar y el gasto.

Véalo en vivo: el mapa de gobernanza en hub.jcardena.com/azure/governance.html

CAPÍTULO DIEZ

Costos: cada número cuadra



Lo esencial: cada euro o dólar que gasta el entorno tiene un responsable que lo esperaba, un límite que alguien acordó y un registro que cuadra con la factura. El costo no es una sorpresa mensual que finanzas tenga que explicar. Es una capa de garantía, gobernada por los mismos contratos que la seguridad.

En el libro fundacional de la serie, el contrato tiene una cláusula de presupuesto: cuánto puede gastar una puerta, por ejecución y por período, y qué ocurre al llegar al límite. En Azure, las puertas son las suscripciones y los grupos de recursos, y la cláusula se escribe con etiquetas, presupuestos, alertas y compromisos. El lema de esta capa la describe con exactitud: cada número cuadra. Un error del 3 % en un informe de costos es el tipo de fallo silencioso que hace que los líderes dejen de confiar en toda la plataforma.

Empezar por la responsabilidad: etiquetas con significado

El capítulo cuatro dio a cada carga de trabajo su propia suscripción por entorno, lo que ya responde a la mayoría de las preguntas de costos: la suscripción es la línea de la factura. Las etiquetas responden al resto. Requerimos un conjunto breve, que las directivas del capítulo seis hacen cumplir y que se define en el diccionario de etiquetas del apéndice: `owner`, `costCenter`, `environment`, `workload` y `dataClassification`. El proceso de aprovisionamiento las asigna a la suscripción y a sus grupos de recursos. Cost Management puede entonces agrupar y filtrar el gasto por etiqueta y, en las cuentas de Contrato Enterprise y de Contrato de cliente de Microsoft, su configuración de herencia de etiquetas puede aplicar las etiquetas de la suscripción y del grupo de recursos a los registros de uso, de modo que el gasto de un recurso creado sin etiquetas quede imputado igualmente a la partida correcta.

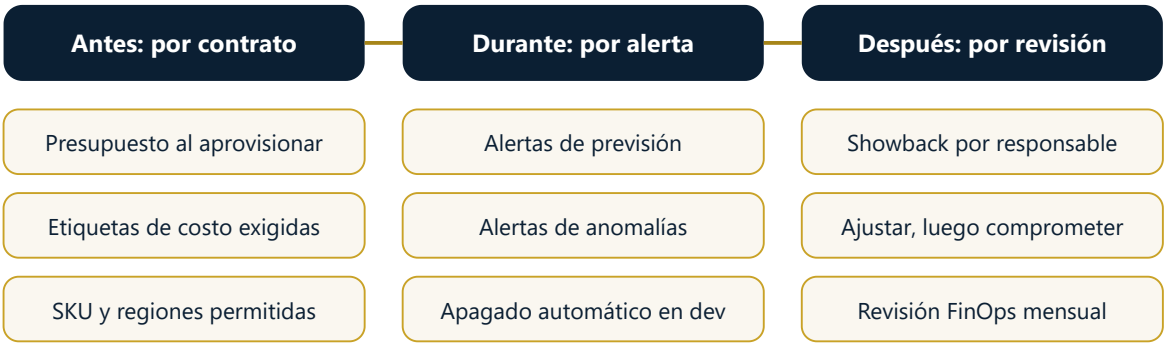
La visibilidad del gasto por responsable (showback) va primero: cada responsable ve su propio gasto, cada mes, en la misma vista. La refacturación (chargeback), en la que el costo pasa a una partida presupuestaria, puede venir después, una vez que los números inspiran

confianza. Intentar la refacturación con números en los que nadie confía genera discusiones, no ahorros.

Los costos compartidos de la plataforma también necesitan una regla: de lo contrario, el hub, el firewall y el área de trabajo central se convierten en la línea de la que nadie es responsable. En las cuentas de Contrato Enterprise y de Contrato de cliente de Microsoft, las reglas de asignación de costos de Cost Management pueden repartir el costo de una suscripción, un grupo de recursos o una etiqueta compartidos entre las cargas de trabajo de destino, con porcentajes fijos o en proporción a su propio gasto. La asignación cambia lo que muestran el análisis de costos, los presupuestos y las exportaciones, no la factura, y no se aplica a compras como las reservas y los planes de ahorro. Para herramientas externas a Azure, programe exportaciones de Cost Management en formato FOCUS (FinOps Open Cost and Usage Specification), para que finanzas pueda combinar el costo de Azure con los datos de otros proveedores en un mismo esquema.

FIGURA 10.1

Controles de costos antes, durante y después del gasto



El incidente de costo más barato es el que el contrato rechazó antes de que existiera el recurso.

Tres momentos, tres tipos de control. Las directivas y el aprovisionamiento detienen los errores evidentes; las alertas detectan las sorpresas en uno o dos días; la revisión convierte los patrones en compromisos y en reglas nuevas.

Presupuestos: un acuerdo con aviso temprano

Un presupuesto de Cost Management puede definirse en el ámbito de un grupo de administración, una suscripción o un grupo de recursos (y en ámbitos de facturación, según el tipo de acuerdo de facturación). Se restablece cada mes, trimestre o año, y envía notificaciones cuando el costo real o el costo previsto supera un umbral porcentual. Un solo presupuesto puede tener hasta cinco umbrales.

Dos hechos determinan cómo los usamos. Primero, **un presupuesto no detiene nada**; Microsoft deja claro que los recursos no se ven afectados y el consumo continúa. Segundo, en las cuentas de Contrato Enterprise y de Contrato de cliente de Microsoft, los datos de costos suelen llegar en un plazo de 8 a 24 horas (en pago por uso pueden tardar hasta 72), y los presupuestos se evalúan aproximadamente una vez al día, así que un presupuesto es un aviso temprano, no un interruptor automático. Si necesita automatización al alcanzar un umbral, un presupuesto en el ámbito de una suscripción o de un grupo de recursos puede invocar un grupo de acciones de Azure Monitor, por ejemplo para apagar las máquinas virtuales de desarrollo.

Nuestro estándar: cada suscripción recibe un presupuesto en el momento del aprovisionamiento, con una alerta de previsión al 100 % y alertas de costo real al 80 % y al 100 %, enviadas a la dirección de la etiqueta de responsable y al canal de costos de la plataforma. El presupuesto es código, implementado junto con la suscripción:

```
targetScope = 'subscription'

param amount int
param startDate string            // primer día de un mes, p. ej. '2027-01-01'
param contactEmails array

resource budget 'Microsoft.Consumption/budgets@2023-05-01' = {
  name: 'budget-monthly'
  properties: {
    category: 'Cost'
    amount: amount
    timeGrain: 'Monthly'
    timePeriod: { startDate: startDate }
    notifications: {
      actual80: {
        enabled: true
        operator: 'GreaterThanOrEqualTo'
        threshold: 80
        thresholdType: 'Actual'
        contactEmails: contactEmails
      }
      actual100: {
        enabled: true
        operator: 'GreaterThanOrEqualTo'
        threshold: 100
        thresholdType: 'Actual'
        contactEmails: contactEmails
      }
      forecast100: {
        enabled: true
        operator: 'GreaterThan'
        threshold: 100
        thresholdType: 'Forecasted'
        contactEmails: contactEmails
      }
    }
  }
}
```

Alertas de anomalías: el detector de sorpresas

Los presupuestos detectan el gasto excesivo sostenido. Las anomalías detectan el pico repentino: una configuración de escalado que se quedó alta, un clúster de pruebas que nunca se detuvo. Cost Management evalúa cada suscripción a diario, compara el uso del día con una previsión construida a partir de los 60 días anteriores y se ejecuta unas 36 horas después del final del día para que los datos estén completos. Una regla de alerta de anomalías envía un correo una sola vez, en el momento de la detección, con los grupos de recursos que más cambiaron.

Las reglas de alerta de anomalías solo se crean en el ámbito de la suscripción, requieren Cost Management Contributor (o Contributor u Owner) en esa suscripción y están limitadas a cinco por suscripción. Las alertas se envían con el acceso actual de quien creó la regla, de modo que una regla creada por una persona cuyo rol caduca después en Privileged Identity Management (capítulo cinco) deja de avisar. La recomendación de Microsoft para ese caso es crear la regla con una entidad de servicio mediante la API de Scheduled Actions. Hacemos exactamente eso, desde el pipeline de aprovisionamiento.

Compromisos: para producción, después de ajustar el tamaño

Azure ofrece dos formas de comprometerse por uno o tres años a cambio de tarifas más bajas. Una **reserva** compromete un tipo de recurso y una configuración en una región; para las máquinas virtuales, la flexibilidad de tamaño de instancia permite que el descuento se aplique a otros tamaños del mismo grupo. Ahorra más cuando la carga de trabajo es estable. Un **plan de ahorro** compromete un gasto fijo por hora en los servicios y regiones aptos: cómputo, más un plan de ahorro independiente para determinados servicios de bases de datos; es adecuado para cargas de trabajo que todavía evolucionan.

Los compromisos residen en la jerarquía de facturación, que no es el árbol de grupos de administración. Un Contrato Enterprise tiene una inscripción, departamentos y cuentas; un Contrato de cliente de Microsoft tiene una cuenta de facturación, perfiles de facturación y secciones de factura. Ambas jerarquías son independientes del árbol y se gobiernan con roles de facturación, no con Azure RBAC. Establezca la correspondencia de forma deliberada: los departamentos o las secciones de factura a los responsables de costos, y el derecho a comprar compromisos al responsable de FinOps. Cada reserva o plan de ahorro también tiene un ámbito: un grupo de recursos, una suscripción, un grupo de administración, o compartido en todo el perfil de facturación o la inscripción. El ámbito compartido ofrece la mejor utilización; un ámbito más reducido conviene cuando una unidad de negocio financia la compra.

El orden que recomienda la propia Microsoft es el que seguimos: primero ajustar el tamaño, después intercambiar o canjear las reservas infrautilizadas, comprar reservas nuevas solo para cargas de trabajo estables y bien conocidas, y añadir los planes de ahorro al final, dimensionados a partir de un consumo de referencia ya optimizado. En términos de contrato: los compromisos son una decisión de producción, aprobada en la revisión de FinOps, y nunca se compran para cubrir el desperdicio en desarrollo.

FIGURA 10.2

Reglas de costos por entorno

Regla	Dev	Test	Prod
Presupuesto con alerta de previsión	Sí, ajustado	Sí	Sí
Regla de alerta de anomalías	Sí	Sí	Sí
Apagado automático de VM fuera de horario	Activado por defecto	Activado, con exclusión voluntaria	Desactivado
SKU permitidas (directiva)	Lista reducida	Lista similar a prod	Lista aprobada
Reservas y planes de ahorro	No	No	Tras revisión
Categoría de registros de diagnóstico (capítulo nueve)	audit	audit	audit, más allLogs añadido en el aprovisionamiento

Barato donde se puede, bien pensado donde se debe. Son parámetros de costo, fijados por suscripción en el aprovisionamiento; las barreras de protección del capítulo seis son idénticas en todos los entornos. El nivel de detalle de los registros también es una decisión de costo, y por eso aparece en esta página.

El ritmo de FinOps

Las herramientas encuentran números; las personas deciden. Una vez al mes, el equipo de plataforma, cada responsable de carga de trabajo y el responsable de FinOps miran la misma vista: el gasto frente al presupuesto por suscripción, las anomalías y sus causas, el gasto sin etiquetar, las recomendaciones de costos de Azure Advisor y la utilización de los compromisos. Cada punto termina con un responsable y una fecha. Las causas recurrentes se convierten en directivas: si tres equipos dejaron grandes clústeres de desarrollo en funcionamiento, la lista de SKU permitidas para desarrollo se acorta.

UN EJEMPLO COMPUESTO: LA ALERTA SILENCIOSA

Un entorno tenía alertas de anomalías en todas las suscripciones y, aun así, un pico importante pasó inadvertido durante una semana. Las reglas las había creado un ingeniero cuyo rol elevado tenía una duración limitada. Cuando el rol caducó, las alertas dejaron de enviarse, sin ningún error en ninguna parte. Volver a crear las reglas con una identidad de pipeline y añadir a la revisión mensual el punto "quien creó la regla de alerta todavía tiene acceso" resolvió el problema.

> *Un presupuesto no es un límite. Es una promesa con un aviso temprano. El límite es el contrato que usted hace cumplir antes de gastar el dinero.*

LISTA DE VERIFICACIÓN DEL CONTRATO

- Cada suscripción tiene etiquetas de responsable, centro de costo, entorno y carga de trabajo, que las directivas hacen cumplir.
- Cada suscripción tiene un presupuesto con alertas de costo real y de previsión, implementado como código en el aprovisionamiento.
- Existen reglas de alerta de anomalías en todas las suscripciones, creadas por una identidad de pipeline que no caduca.
- Las reservas y los planes de ahorro se compran solo para producción con el tamaño ya ajustado, tras una revisión.
- Una revisión mensual de FinOps cierra cada punto con un responsable y una fecha.

Véalo en vivo: la página de costos en hub.jcardena.com/azure/governance-cost.html

PARTE V · OPERAR

CAPÍTULO ONCE

Implementar por contrato: infraestructura como código



Lo esencial: en producción, nadie cambia la infraestructura a mano. Cada cambio es código, revisado por una persona, previsualizado por la plataforma, implementado por una identidad de pipeline que no tiene contraseña y protegido después para que el portal no pueda deshacerlo en silencio. Aquí el modelo es la pull request: propone, y el contrato decide.

En las partes I a IV se describió cómo es un entorno gobernado. La parte V trata de mantenerlo así mientras decenas de equipos lo cambian cada semana. Este capítulo trata la puerta por la que deberían llegar casi todos los cambios: el pipeline de implementación. El capítulo siguiente trata de las personas y el ritmo que hacen funcionar todo el sistema.

Elegir un lenguaje por capa y usar módulos verificados

Tanto Bicep como Terraform tienen buen soporte en Azure. Al contrato no le importa cuál elija; le importa que lo elija de forma deliberada y que no los mezcle para los mismos recursos. En un entorno de producción típico, la capa de plataforma (grupos de administración, directivas, red hub) y la capa de cargas de trabajo pueden usar herramientas distintas, pero cada recurso tiene exactamente una fuente de verdad.

No escriba cada recurso desde cero. **Azure Verified Modules** (AVM) es una iniciativa de Microsoft que establece un único estándar de calidad para los módulos de infraestructura en Bicep y Terraform. Los módulos de recursos implementan un único recurso con sus extensiones habituales, como la configuración de diagnóstico, los bloqueos, las asignaciones de roles y los puntos de conexión privados; los módulos de patrón implementan una arquitectura reutilizable. AVM indica que está a cargo del equipo de ingeniería de Azure y que cuenta con el soporte de Microsoft. Para Bicep, los módulos se publican en el registro público y se referencian por versión:

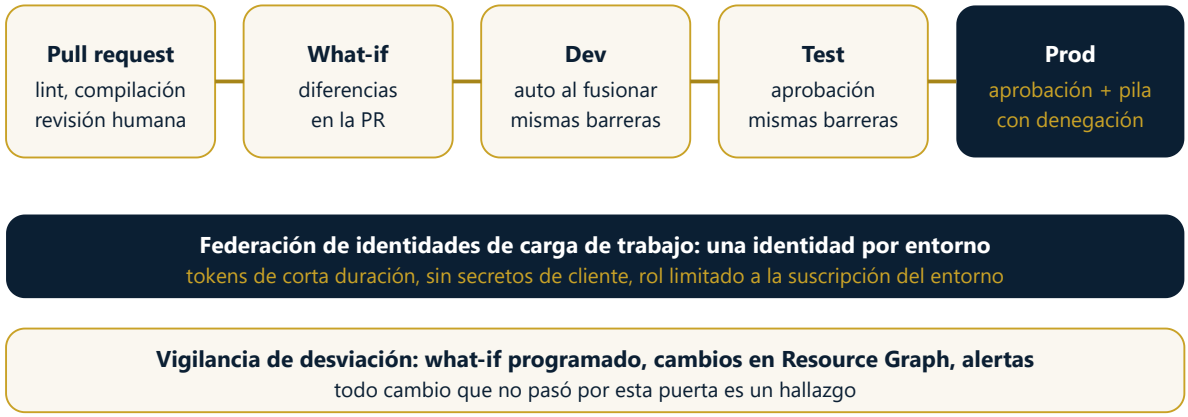
```
param kvName string

// Módulo de recursos de AVM, fijado a una versión publicada (la actual en el momento de
escribir).
module kv 'br/public:avm/res/key-vault/vault:0.14.2' = {
  name: 'kv-deploy'
  params: {
    name: kvName
    enableRbacAuthorization: true
    enablePurgeProtection: true
    publicNetworkAccess: 'Disabled'
  }
}
```

Fije las versiones y actualícelas de forma deliberada, mediante la misma revisión que cualquier otro cambio. Un módulo que se actualiza solo a "latest" introduce un cambio que nadie revisó.

FIGURA 11.1

La puerta de implementación, de la pull request a producción



Cinco puertas, una identidad por entorno, una vigilancia posterior. Las personas revisan la intención; la plataforma previsualiza el efecto; las aprobaciones protegen la promoción; la configuración de denegación protege el resultado.

Pipelines sin secretos

El capítulo cinco dijo: nada de claves compartidas. Es en los pipelines donde más se incumple esa regla, porque un secreto de entidad de servicio pegado en una variable del pipeline funciona el primer día y se filtra el día cuatrocientos. La **federación de identidades de carga de trabajo** elimina el secreto. La plataforma del pipeline emite un

token de corta duración para un repositorio, una rama o un entorno concretos; Microsoft Entra ID confía en ese emisor mediante una credencial federada y canjea el token por un token de acceso de Azure.

Azure DevOps recomienda ahora la federación de identidades de carga de trabajo para las conexiones de servicio de Azure Resource Manager, con un registro de aplicación o con una identidad administrada asignada por el usuario, y puede convertir las conexiones existentes basadas en secretos. GitHub Actions usa el mismo mecanismo mediante OpenID Connect con la acción de inicio de sesión de Azure. En cualquier caso, nuestras reglas son las mismas:

- Una identidad por entorno, para que un pipeline de desarrollo no pueda tocar producción.
- La credencial federada está vinculada a la rama o al entorno protegidos, no a cualquier rama.
- Asignaciones de roles en el ámbito más bajo que funcione, con los roles integrados del capítulo cinco. Nunca conceda acceso a "todos los pipelines" en una conexión de producción.

What-if: la vista previa forma parte de la revisión

Un revisor que lee Bicep ve la intención. Un revisor que lee la salida de what-if ve el efecto: qué recursos se crearán, modificarán o eliminarán, y qué propiedades cambian. Azure Resource Manager ofrece la operación what-if en el ámbito del grupo de recursos, la suscripción, el grupo de administración y el inquilino (`az deployment group what-if` y sus equivalentes), y la CLI puede devolver JSON con `--no-pretty-print` para que un pipeline lo inspeccione.

Ejecutamos what-if en cada pull request sobre el entorno de destino y publicamos el resumen en la revisión. Dos advertencias de la documentación de Microsoft permiten usar esta puerta con rigor: what-if puede informar de "ruido", propiedades que parecen cambiar pero no lo harán, y no puede evaluar algunas expresiones, como `utcNow()` o las referencias a recursos externos a la plantilla. Trate la salida como evidencia para una persona y deje que la puerta bloquee el cambio automáticamente solo ante señales claras, como una eliminación inesperada en producción.

Pilas de implementación: proteger lo que se implementó

Una pila de implementación es un recurso de Azure que administra un conjunto de recursos como una sola unidad. Registra lo que administra, decide qué ocurre con los recursos que se quitan de la plantilla (`detachAll`, `deleteResources` o `deleteAll`) y puede aplicar una **configuración de denegación** que bloquea los cambios de todos los demás. Los modos

son `none`, `denyDelete` y `denyWriteAndDelete`. Las pilas pueden crearse en el ámbito del grupo de recursos, de la suscripción o del grupo de administración, y dos roles integrados las controlan: Azure Deployment Stack Contributor y Azure Deployment Stack Owner.

```
az deployment group what-if \
  --resource-group rg-claims-prod \
  --template-file main.bicep \
  --parameters environment=prod

az stack group create \
  --name claims-prod \
  --resource-group rg-claims-prod \
  --template-file main.bicep \
  --parameters environment=prod \
  --action-on-unmanage detachAll \
  --deny-settings-mode denyWriteAndDelete \
  --deny-settings-excluded-principals "$EXCLUDED_GROUP_ID"
```

Hay dos detalles importantes. La configuración de denegación solo se aplica al plano de control, igual que los bloqueos del capítulo ocho; no impide operaciones del plano de datos, como escribir un blob o un secreto. Y la lista de entidades excluidas admite como máximo cinco entradas, así que siga la recomendación de Microsoft y excluya un grupo de Microsoft Entra que contenga la identidad del pipeline, los administradores de emergencia (break-glass) y las identidades de corrección de las directivas. Si olvida estas últimas, sus directivas DeployIfNotExists de los capítulos siete y nueve serán rechazadas en los recursos protegidos.

Las directivas también son código, y se prueban

Las definiciones de directivas, las iniciativas, las asignaciones y las exenciones se guardan en el mismo repositorio y en el mismo pipeline que todo lo demás. Cada cambio se versiona y se revisa, y la reversión es una nueva implementación del commit anterior. Antes de que un cambio de directiva o de rol llegue al árbol de producción, pruébelo. La guía de Microsoft sobre zonas de aterrizaje describe un enfoque canary: una jerarquía duplicada de grupos de administración con sus propias suscripciones y sus propias identidades de pipeline, donde los cambios se implementan primero sobre cargas de trabajo de ejemplo. Microsoft señala que es opcional y que se adapta a organizaciones con una gestión de cambios sólida. Los entornos más pequeños pueden basarse en el escalonamiento del capítulo seis: primero DoNotEnforce, después un selector de recursos reducido y luego el ámbito completo. Herramientas de código abierto como Enterprise Policy as Code (EPAC) o los módulos de zona de aterrizaje de Azure pueden encargarse de la mecánica de implementación.

Desviación: cambios que no pasaron por la puerta

Incluso con todos los controles anteriores, algo cambiará fuera del pipeline: una corrección de emergencia, un clic en el portal de alguien con acceso elevado. Buscamos la desviación de tres formas. Un what-if programado sobre cada pila de producción informa de cualquier diferencia respecto al código. Azure Resource Graph conserva 14 días de cambios en la configuración de los recursos para la investigación. Una alerta del registro de actividad, del capítulo nueve, se dispara ante operaciones de escritura en producción cuyo autor no es una identidad de pipeline. Cada hallazgo se resuelve de una de dos maneras: el cambio se incorpora al código, o se vuelve a implementar el código para sobrescribir el cambio.

Sin cambios manuales en producción no significa sin personas en producción. Las personas tienen Reader de forma predeterminada y elevan sus permisos mediante Privileged Identity Management (capítulo cinco) para los incidentes. Una activación es un evento de acceso, registrado por PIM. Cualquier cambio manual hecho durante ella es una desviación: recibe un registro de cambio y se incorpora al código o se revierte en un plazo acordado.

UN EJEMPLO COMPUESTO: LA CORRECCIÓN QUE SIEMPRE VOLVÍA

Un ingeniero de guardia aumentó la capacidad de una base de datos desde el portal durante un incidente. La siguiente implementación rutinaria la devolvió a su valor anterior, y el incidente regresó. La causa no fue el ingeniero ni el pipeline. Fue un paso que faltaba: los cambios de emergencia no se incorporaban al código. El equipo añadió la comprobación de desviación y una regla según la cual el incidente no se cierra hasta que se fusiona la pull request.

> *La infraestructura como código no consiste en escribir menos. Consiste en hacer que cada cambio pase por una puerta que lo revisa, lo previsualiza, lo registra y lo protege.*

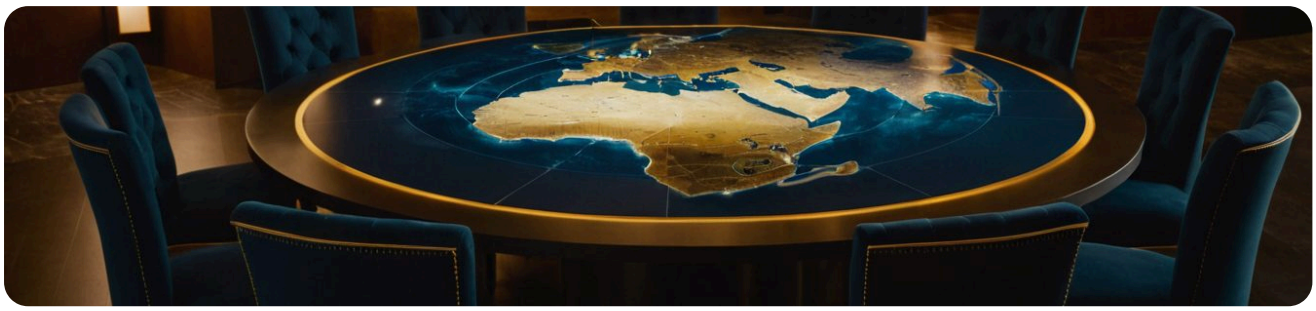
LISTA DE VERIFICACIÓN DEL CONTRATO

- Cada recurso tiene una única fuente de verdad en el código; las versiones de los módulos están fijadas.
- Los pipelines usan federación de identidades de carga de trabajo, una identidad por entorno, sin secretos.
- Cada pull request muestra un what-if sobre su entorno de destino.
- La promoción a pruebas y a producción requiere una aprobación; los recursos de producción están en pilas con configuración de denegación.
- La desviación se detecta de forma programada y cada hallazgo se cierra en el código.
- Los cambios de directivas se versionan, se escalonan o se prueban en una jerarquía canary y se publican mediante el pipeline.

Véalo en vivo: la página de directivas en hub.jcardena.com/azure/governance-policy.html

CAPÍTULO DOCE

El modelo operativo de gobernanza



Lo esencial: la gobernanza no es un conjunto de configuraciones que se implementa una vez. Es un equipo pequeño, un reparto claro de quién decide qué, un ritmo regular y un cuadro de mando de una página que le dice a la dirección si el entorno está cumpliendo sus promesas. Sin todo ello, cada control de este libro se degrada poco a poco.

En los once capítulos anteriores se construyeron los contratos: inquilino, árbol, suscripciones, roles, directivas, red, postura, visibilidad, costo e implementación. Este capítulo responde la pregunta que todo CIO hace al final de una revisión de diseño: ¿quién opera esto, con qué frecuencia y cómo sabré que funciona? También ofrece un plan de 30, 60 y 90 días para el caso que la mayoría de los lectores tiene en realidad: no un inquilino nuevo y limpio, sino un entorno existente que creció sin un plan.

Dos tipos de equipo, una frontera

El modelo de zonas de aterrizaje de Azure separa un **equipo de plataforma** de los **equipos de carga de trabajo**. El equipo de plataforma es responsable de todo lo que está bajo el grupo de administración Platform del capítulo tres (identidad, administración, conectividad), del conjunto de directivas del capítulo seis, del proceso de aprovisionamiento de suscripciones del capítulo cuatro y de los pipelines que los implementan. Los equipos de carga de trabajo son responsables de lo que hay dentro de las suscripciones de su zona de aterrizaje: su red spoke, sus servicios, sus datos, sus alertas y su gasto.

La frontera entre ellos es el contrato. Los equipos de carga de trabajo avanzan rápido dentro de él sin pedir permiso. Cuando necesitan algo fuera de él (una nueva región, un punto de conexión público, una SKU que no está en la lista), lo piden por una sola puerta: una exención o un cambio al contrato, registrado con un responsable, un motivo y una fecha de caducidad.

FIGURA 12.1

RACI para el entorno gobernado

Actividad	Plataforma	Carga de trabajo	Seguridad	FinOps	Comité de dirección
Grupos de administración y conjunto de directivas	R/A	C	C	C	I
Aprovisionamiento de suscripciones	R/A	C	I	C	I
Red central (hub), DNS, firewall	R/A	I	C	I	I
Recursos en una zona de aterrizaje	C	R/A	C	I	I
Hallazgos de postura en una zona de aterrizaje	C	R	A	I	I
Presupuestos y compromisos	R	C	I	A	I
Exenciones de directivas	R	C	A	C	I
Aplicación de revisiones en máquinas de carga de trabajo	C	R/A	C	I	I
Cambios al propio contrato	R	C	C	C	A

R responsable de ejecutar, **A** responsable final (rinde cuentas), **C** consultado, **I** informado. Un único responsable final por fila. El comité de dirección es un grupo pequeño presidido por el CIO o su delegado.

El ritmo

- **Diario, automatizado.** Las directivas evalúan los recursos, Defender analiza la postura, se ejecuta la detección de anomalías y las alertas llegan a sus responsables. Nadie se reúne.
- **Semanal, 30 minutos, equipo de plataforma.** Nuevas solicitudes de exención, hallazgos de desviación del capítulo once, tareas de corrección fallidas, solicitudes de aprovisionamiento.
- **Mensual, una hora, plataforma más responsables de carga de trabajo, seguridad y FinOps.** El cuadro de mando, la revisión de FinOps del capítulo diez, los principales controles de postura del capítulo ocho, las exenciones que vencen este mes.

- **Trimestral, comité de dirección.** Cambios al contrato: nuevas directivas que pasan de auditar a denegar, nuevas regiones o servicios permitidos, compras de compromisos, resultados de pruebas de restauración y conmutación por error.

El cuadro de mando de una página

Los líderes no necesitan cincuenta paneles. Necesitan unas diez cifras, cada una vinculada a una garantía de este libro, cada una con un objetivo y una tendencia. Cada una de las cifras siguientes puede calcularse a partir de los datos de cumplimiento de Azure Policy, Defender for Cloud, Cost Management, Azure Resource Graph o el área de trabajo central.

FIGURA 12.2

Cuadro de mando: una fila por garantía

Capa	Medida	Fuente	Objetivo de ejemplo
Contratos	Cumplimiento de directivas, ámbito de producción	Azure Policy	En aumento, fijado por el comité de dirección
Contratos	Exenciones vencidas	Exenciones de directivas	Cero
Seguridad	Puntuación de seguridad (modelo indicado)	Defender for Cloud	En aumento cada mes
Seguridad	Roles privilegiados permanentes en manos de personas	Entra ID, PIM	Solo cuentas de emergencia
Seguridad	Cargas de producción con restauración probada este trimestre	Registro de revisión	Todas
Visibilidad	Suscripciones que envían registros de actividad al área de trabajo central	Resource Graph	Todas
Visibilidad	Cambios en producción no hechos por un pipeline	Registro de actividad	Cada uno explicado
Costo	Suscripciones con presupuesto y alerta de anomalía	Cost Management	Todas
Costo	Gasto sin etiqueta de responsable	Análisis de costos	Bajando hasta casi cero
Costo	Gasto frente a presupuesto, por responsable	Cost Management	Dentro del rango acordado

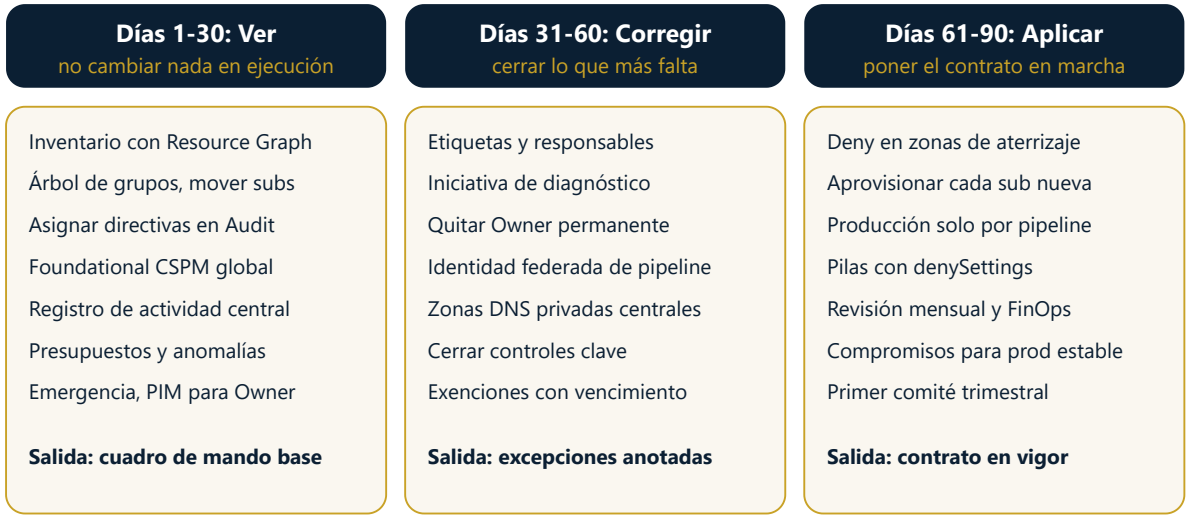
Los objetivos los fija su comité de dirección, no este libro. Lo importante es que cada cifra exista, se calcule de la misma forma cada mes y tenga un responsable.

Plan de 30, 60 y 90 días para un entorno existente

La mayoría de los entornos ya tienen decenas de suscripciones, responsables que nadie recuerda y algunos puntos de conexión públicos que "deben quedarse". El orden que funciona es siempre el mismo: primero ver, luego corregir y después hacer cumplir. Activar directivas de denegación el primer día interrumpe implementaciones y consume la confianza que usted necesitará durante los siguientes noventa días.

FIGURA 12.3

Ver, corregir, hacer cumplir



Auditar antes de denegar, siempre. Los resultados de auditoría del primer mes le indican qué reglas de denegación romperán algo, de modo que pueda corregir o conceder exenciones primero y después hacer cumplir las reglas sin sorpresas.

Tres prácticas permiten que el plan resista el contacto con un entorno real. Primero, publique el cuadro de mando de referencia el día 30 aunque sus cifras sean malas; una cifra mala pero honesta es el punto de partida que la dirección necesita. Segundo, dé a cada excepción una fecha de caducidad, no una promesa; la revisión semanal hace el seguimiento de esas fechas. Tercero, pase las reglas de auditar a denegar de una en una, empezando por las que cubren más riesgo y rompen menos implementaciones, normalmente el acceso de red público en servicios de datos y las regiones permitidas.

Incorporación de una nueva carga de trabajo

1. El responsable de la carga de trabajo solicita zonas de aterrizaje mediante el formulario de aprovisionamiento: nombre, responsable, centro de costo, clase de datos, entornos.
2. El aprovisionamiento crea una suscripción por entorno bajo el grupo de administración correcto, con etiquetas, presupuesto, alerta de anomalía, red spoke, configuración de diagnóstico y planes de Defender ya establecidos.
3. El equipo de plataforma concede a los grupos del equipo sus roles mediante PIM y crea una identidad federada de pipeline por entorno.
4. El equipo lee el resumen del contrato: qué se deniega, qué se audita, cómo solicitar una exención.
5. La carga de trabajo aparece en el cuadro de mando desde su primer día.

El contrato evoluciona

Microsoft cambia el nombre de servicios, agrega definiciones de directivas y cambia valores predeterminados; este libro mencionó varios de esos cambios de paso. El contrato se mantiene al día porque tiene un responsable y una revisión, no porque alguien lo recuerde. Cada trimestre, el comité de dirección revisa las nuevas directivas integradas, las características retiradas y la lista de exenciones, y cada cambio se publica por el mismo pipeline que todo lo demás.

> *La confianza, ganada en cada capa, no es un lema que se imprime. Es un cuadro de mando que usted puede mostrar cada mes, con las mismas cifras calculadas de la misma forma.*

LISTA DE VERIFICACIÓN DEL CONTRATO

- Las responsabilidades de plataforma y de carga de trabajo están escritas en una matriz RACI con un único responsable final por fila.
- Las revisiones semanales, mensuales y trimestrales están en el calendario con asistentes designados.
- Existe un cuadro de mando de una página, con fuentes y responsables para cada cifra.
- Los entornos existentes siguen la secuencia ver, corregir y hacer cumplir; ninguna regla de denegación entra en vigor antes de revisar sus resultados de auditoría.
- Las nuevas cargas de trabajo llegan solo mediante el aprovisionamiento, ya dentro del contrato.

Véalo en vivo: el mapa de gobernanza en hub.jcardena.com/azure/governance.html

APÉNDICE

Apéndice: Plantillas



Estas plantillas condensan el libro en una sola mesa de trabajo. Cópielas, cambie los nombres, discuta las celdas con su equipo y mantenga el resultado bajo control de versiones junto al código que gobierna. Una plantilla con la que nadie está en desacuerdo es una plantilla que nadie ha leído.

Cada plantilla remite al capítulo que la explica. Cuando una celda nombra un rol o una directiva integrados de Azure, compruebe el nombre actual en la documentación de Microsoft antes de confiar en él; los nombres y los valores predeterminados cambian, y lo que importa es el patrón.

A.1 Mapa de grupos de administración y suscripciones

La forma de los capítulos tres y cuatro: un árbol poco profundo, la plataforma separada de las cargas de trabajo, una suscripción por carga de trabajo y por entorno. Sustituya las cargas de trabajo de ejemplo por las suyas.

FIGURA A.1

Mapa de grupos de administración y suscripciones



Las directivas y los roles se heredan hacia abajo en el árbol. Asigne las reglas generales en Organization root y las barreras de protección en Landing zones, idénticas para cada entorno. Los parámetros de costo y las obligaciones exclusivas de producción van en las suscripciones de carga de trabajo durante el aprovisionamiento. Mantenga el árbol poco profundo; tres o cuatro niveles bajo la raíz bastan para la mayoría de los entornos.

A.2 Matriz de roles: perfil por entorno

Del capítulo cinco: asignar a grupos, no a personas; el ámbito más bajo que funcione; elevación con límite de tiempo mediante Privileged Identity Management (PIM) para todo lo que pueda cambiar producción. "Apto" (eligible) significa que el rol se activa mediante PIM con un motivo y una fecha de caducidad.

Perfil	Dev	Test	Prod
Desarrollador de carga de trabajo	Contributor (apto, sin aprobación)	Reader; Contributor (apto)	Reader; sin escritura
Líder de carga de trabajo	Contributor (apto)	Contributor (apto)	Contributor (apto, con aprobación)
Identidad de pipeline (una por entorno)	Contributor en su suscripción	Contributor en su suscripción	Contributor en su suscripción
Entorno de ejecución de la aplicación	Identidad administrada solo con roles de datos, por ejemplo Key Vault Secrets User		

Ingeniero de plataforma	Owner apto en el grupo de administración Landing zones; roles aptos separados en el grupo de administración Platform o sus suscripciones, con privilegio mínimo (aprobación obligatoria, al menos dos aprobadores configurados)
Administrador de acceso	Role Based Access Control Administrator (apto, con condiciones que limitan qué roles puede asignar)
Equipo de seguridad	Security Reader permanente; Security Admin (apto)
Líder de FinOps	Cost Management Reader permanente; Cost Management Contributor apto para cambios de presupuesto; los presupuestos y las reglas de alerta de anomalías los crea la identidad del pipeline de aprovisionamiento (capítulo diez)
Auditor	Reader, revisión de acceso con límite de tiempo
Cuentas de acceso de emergencia	Global Administrator en Microsoft Entra ID, usado solo en emergencias como describe el capítulo dos; cada inicio de sesión genera una alerta

Los pipelines que además asignan roles o implementan pilas de implementación con configuración de denegación necesitan más que Contributor. Conceda exactamente eso (por ejemplo, una asignación restringida de Role Based Access Control Administrator, o Azure Deployment Stack Owner) y registre el motivo.

A.3 Conjunto inicial de directivas con efectos objetivo

De los capítulos seis a diez. Las barreras de protección son las mismas para desarrollo, pruebas y producción. Las reglas Deny se asignan una sola vez en el grupo de administración Landing zones; Modify, DeployIfNotExists y las líneas base de auditoría se asignan en la raíz intermedia, de modo que también quedan cubiertas las suscripciones de plataforma (capítulos seis y nueve). El único conjunto deliberadamente más laxo es Sandbox. En un entorno existente, cada fila Deny empieza en Audit (o con el modo de aplicación establecido en DoNotEnforce) durante las fases de ver y corregir del plan de 30, 60 y 90 días (capítulo doce), y después pasa al efecto objetivo en una fecha fijada en el calendario. DINE significa DeployIfNotExists.

Regla (intención)	Punto de partida integrado	Sandbox	Landing zones: dev, test y prod (objetivo)
Recursos solo en regiones aprobadas	Allowed locations	Deny	Deny
Etiquetas obligatorias presentes	Require a tag on resources	Audit	Deny
Etiquetas heredadas de la suscripción	Inherit a tag from the subscription if missing	Modify	Modify

Bloquear tipos de recursos de riesgo	Not allowed resource types	Audit	Deny
Tamaños de máquina virtual aprobados	Allowed virtual machine size SKUs	Audit	Deny, asignada por suscripción durante el aprovisionamiento con una lista por entorno
Cada subred de carga de trabajo tiene un grupo de seguridad de red (salvo subredes especiales como GatewaySubnet y AzureFirewallSubnet)	Subnets should be associated with a Network Security Group	AuditIfNotExists	AuditIfNotExists
Aplicaciones web públicas detrás de un WAF	Directivas integradas de WAF para Front Door y Application Gateway	Sin asignar	Audit, luego Deny (Online)
Máquinas virtuales de producción con copia de seguridad	Azure Backup should be enabled for Virtual Machines	Sin asignar	AuditIfNotExists; configurar en las suscripciones de producción
Sin IP públicas en las NIC de las máquinas virtuales	Network interfaces should not have public IPs	Audit	Deny
Acceso de red público desactivado en servicios de datos	Por servicio, integrada donde exista	Audit	Deny
Sin zonas DNS `privatelink` en las redes spoke	Personalizada o referencia de zona de aterrizaje	Sin asignar	Deny
Registros DNS de puntos de conexión privados	Configure Azure PaaS services to use private DNS zones (iniciativa de zona de aterrizaje)	Sin asignar	DINE
Registros de recursos al área de trabajo central	Enable audit or allLogs category group resource logging to Log Analytics	DINE (audit)	DINE (audit en la raíz intermedia; allLogs se agrega en las suscripciones de producción durante el aprovisionamiento)
Planes de Defender for Cloud activados	Directivas de configuración de Defender for Cloud	Foundational	Planes según el capítulo ocho

Key Vault usa Azure RBAC y protección de purga	Directivas integradas de Key Vault	Audit	Deny

Cada exención de esta tabla lleva un responsable, un motivo, una categoría (waiver o mitigated) y una fecha de caducidad. Las exenciones caducadas aparecen en el cuadro de mando.

A.4 Diccionario de etiquetas

De los capítulos cuatro y diez. Manténgalo breve; cada etiqueta obligatoria adicional es fricción. Los valores provienen de listas controladas siempre que sea posible.

Etiqueta	Significado	Valor de ejemplo	Obligatoria en	Se hace cumplir con
`owner`	Grupo o rol responsable, no el nombre de una persona	claims-platform-team	Suscripción, grupo de recursos	Directiva deny + herencia
`costCenter`	Código contable que asume el costo	CC-4410	Suscripción, grupo de recursos	Directiva deny + herencia
`environment`	dev, test, prod o sandbox	prod	Suscripción, grupo de recursos	Aprovisionamiento + directiva
`workload`	Nombre corto de la carga de trabajo	claims	Suscripción, grupo de recursos	Aprovisionamiento
`dataClassification`	Mayor sensibilidad contenida: public, internal, confidential o restricted	confidential	Suscripción, grupo de recursos y recursos que contienen datos	Directiva audit primero, luego deny
`rpoRto`	Objetivos de recuperación acordados con el responsable	RPO 15m / RTO 4h	Suscripción de producción	Revisión (capítulo ocho)
`expiresOn`	Fecha de finalización prevista para recursos temporales	2027-03-31	Sandbox, experimentos	Directiva audit + trabajo de limpieza

A.5 Lista de verificación de preparación

Úsela antes de declarar una zona de aterrizaje lista para su primera carga de trabajo de producción. Cada punto corresponde a un capítulo; un "no" es un hallazgo con un responsable y una fecha, no un bloqueo por defecto.

PREPARACIÓN: PLATAFORMA

- Un solo inquilino, cuentas de acceso de emergencia probadas, MFA y acceso condicional en vigor (capítulo dos).
- Árbol de grupos de administración implementado desde código; ninguna suscripción queda bajo la raíz del inquilino (capítulo tres).
- El aprovisionamiento crea suscripciones con etiquetas, presupuesto, alerta de anomalía, red spoke y registro (capítulos cuatro, nueve y diez).
- Ningún Owner de Azure permanente para personas; las cuentas de emergencia solo tienen Global Administrator permanente en Entra; PIM para los roles privilegiados; revisiones de acceso programadas (capítulo cinco).
- Conjunto inicial de directivas asignado, resultados de auditoría revisados, denegación activa en todas las zonas de aterrizaje (capítulo seis).

PREPARACIÓN: CAPAS DE GARANTÍA

- Hub, firewall, resolver y zonas `privatelink` centrales implantados; tráfico de salida registrado (capítulo siete).
- Defender for Cloud activado; modelo de puntuación elegido; estándares de cumplimiento requeridos asignados; bloqueos en los recursos críticos de la plataforma (capítulo ocho).
- RPO, RTO, región de recuperación y una prueba de conmutación por error registrados para cada nivel de producción (capítulo ocho).
- Área de trabajo central que recibe los registros de actividad y de recursos; alertas de la plataforma dirigidas a sus responsables (capítulo nueve).
- Presupuestos, alertas de anomalías y la revisión mensual de FinOps en marcha (capítulo diez).
- Pipelines con federación de identidades de carga de trabajo, what-if en la revisión, pilas que protegen producción (capítulo once).
- RACI, ritmo y cuadro de mando acordados por el comité de dirección (capítulo doce).

> *Las plantillas son donde una filosofía se convierte en hábito. Rellénelas, regístrelas en el repositorio y revíselas según el calendario.*

LISTA DE VERIFICACIÓN DEL CONTRATO

- Cada plantilla anterior está copiada en su repositorio y tiene como propietario a un equipo designado.
- Cada nombre de rol y de directiva integrados en su copia se ha comprobado con la documentación actual de Microsoft.
- La tabla de directivas muestra el efecto objetivo para Sandbox y para las zonas de aterrizaje, y las fechas de paso de auditoría a denegación están en el calendario.
- La lista de verificación de preparación se completa antes de que la primera carga de trabajo de producción entre en servicio.

Véalo en vivo: el mapa de zonas de aterrizaje en hub.jcardena.com/azure/governance-landing-zone.html

LA SERIE

GDCD en Azure

GDCD en Azure aplica el Diseño de Contratos Guiado por la Gobernanza a una plataforma, de principio a fin. El primer libro gobierna el entorno. El segundo entrega IA sobre él.

Libro 1	**Gobernar Azure por contrato**: guía capa por capa para gobernar una plataforma Azure. (Este libro.)
Libro 2	**AI Foundry by Contract** (en inglés): IA gobernada en Azure.

La base del método es *The Contract Decides: Governing AI at Every Door* (en inglés). El mismo método en la puerta del código es *Gobernar Rust por contrato*. Vea cada servicio, modelo y región de Azure en los diagramas en vivo de hub.jcardena.com/azure. Todos los libros se pueden leer gratis en blog.jcardena.com/es/ebooks.

Juan Cardena

Arquitecto de IA empresarial y sistemas agénticos · blog.jcardena.com

Descargue la edición más reciente en blog.jcardena.com/es/ebooks/governing-azure-by-contract.

GDCD en Azure · Libro 1 · Edición 1.1 · La confianza se gana en cada capa.

Traducción al español generada con herramientas de IA a partir del original en inglés y revisada en varias rondas con modelos de IA.