AWS Academy Cloud Foundations

Módulo 9: Arquitectura en la nube

Información general sobre el módulo

Temas

- Marco de Buena Arquitectura de AWS
- Fiabilidad y alta disponibilidad
- AWS Trusted Advisor

Actividades

- Principios de diseño del Marco de Buena Arquitectura de AWS
- Interpretación de las recomendaciones de AWS Trusted Advisor

Revisión de conocimientos

Objetivos del módulo

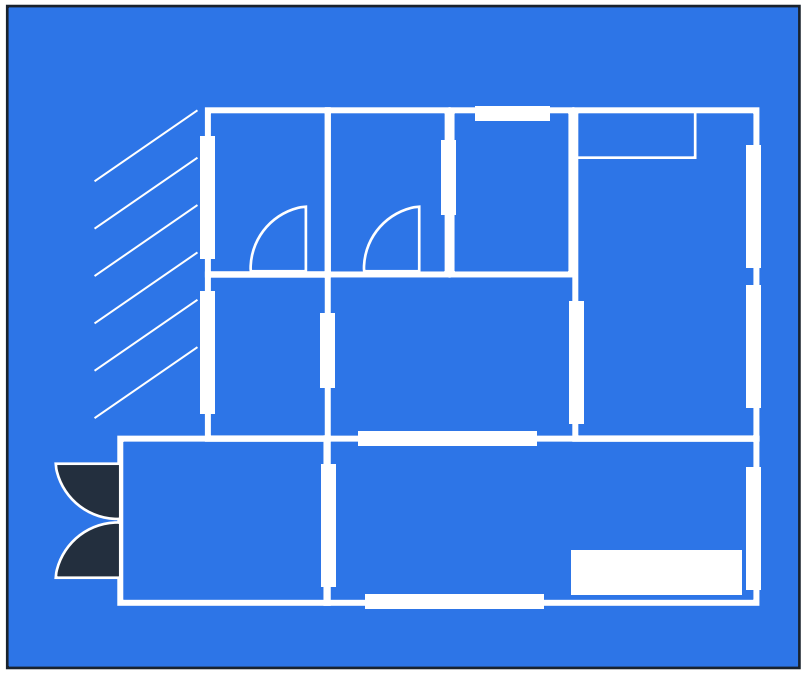
Después de completar este módulo, debería ser capaz de lo siguiente:

- Describir el Marco de Buena Arquitectura de AWS, incluidos los cinco pilares
- Identificar los principios de diseño del Marco de Buena Arquitectura de AWS
- Explicar la importancia de la fiabilidad y la alta disponibilidad
- Identificar cómo AWS Trusted Advisor ayuda a los clientes
- Interpretar las recomendaciones de AWS Trusted Advisor

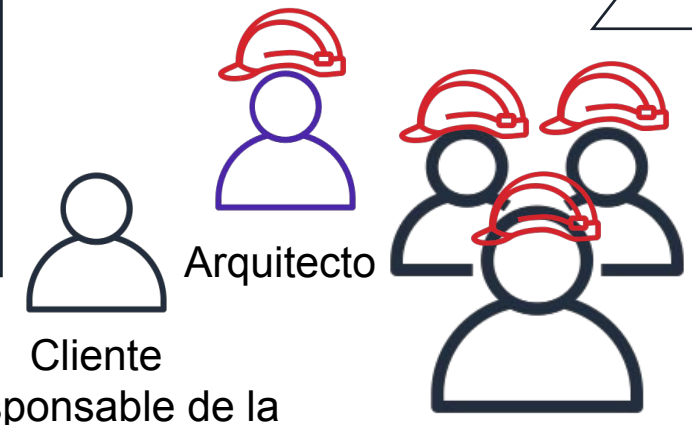
Módulo 9: Arquitectura en la nube

Sección 1: Marco de Buena Arquitectura de AWS

Arquitectura: diseño y creación



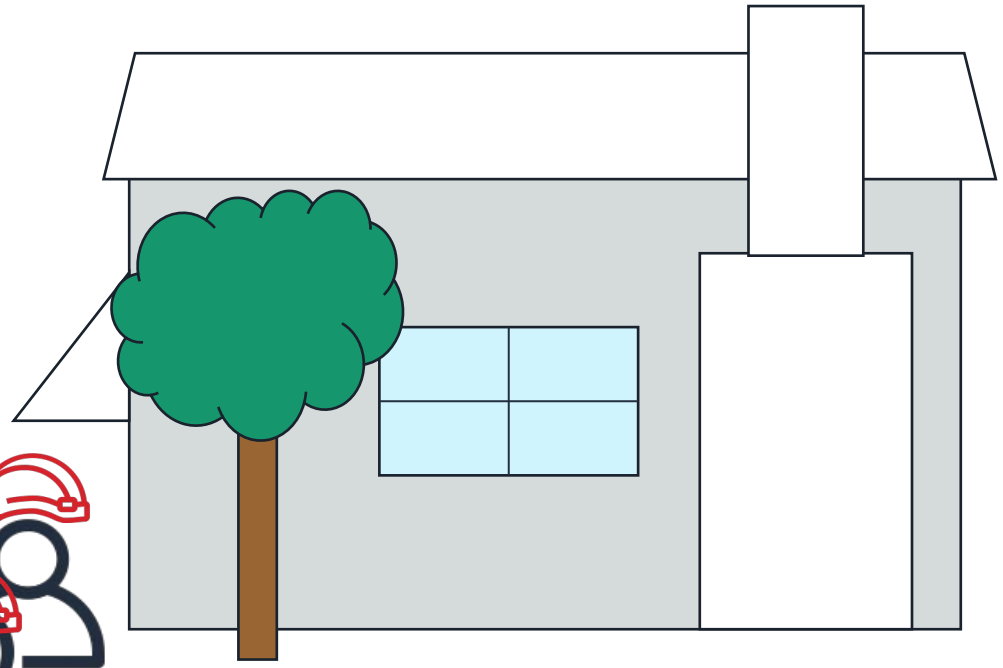
Diseño de la estructura



Cliente (Responsable de la toma de decisiones)

Arquitecto

Personal de creación (Equipo encargado)

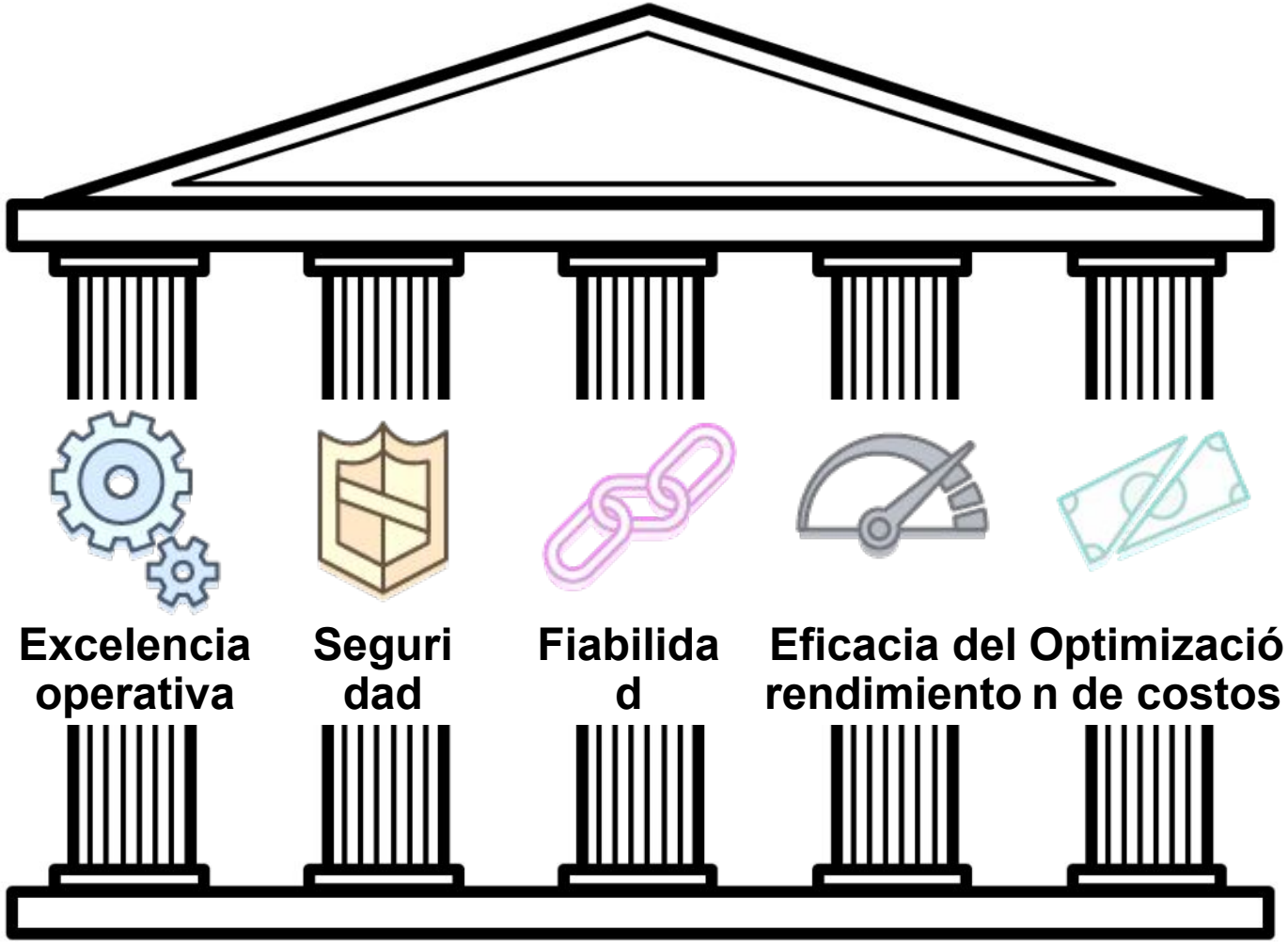


Estructura completa

¿Qué es el Marco de Buena Arquitectura de AWS?

- Una guía para el diseño de infraestructuras que reúnan las siguientes características:
  - ✔ Seguras
  - ✔ De alto desempeño
  - ✔ Resilientes
  - ✔ Eficaces
- Un enfoque uniforme para evaluar e implementar arquitecturas en la nube
- Una forma de brindar prácticas recomendadas que se desarrollaron a partir de las lecciones aprendidas a través de la revisión de arquitecturas de clientes

Pilares del Marco de Buena Arquitectura de AWS



Organización del pilar

Área de prácticas recomendadas

Texto de la pregunta

Contexto de la pregunta

Prácticas recomendadas

Administración de identidad y acceso

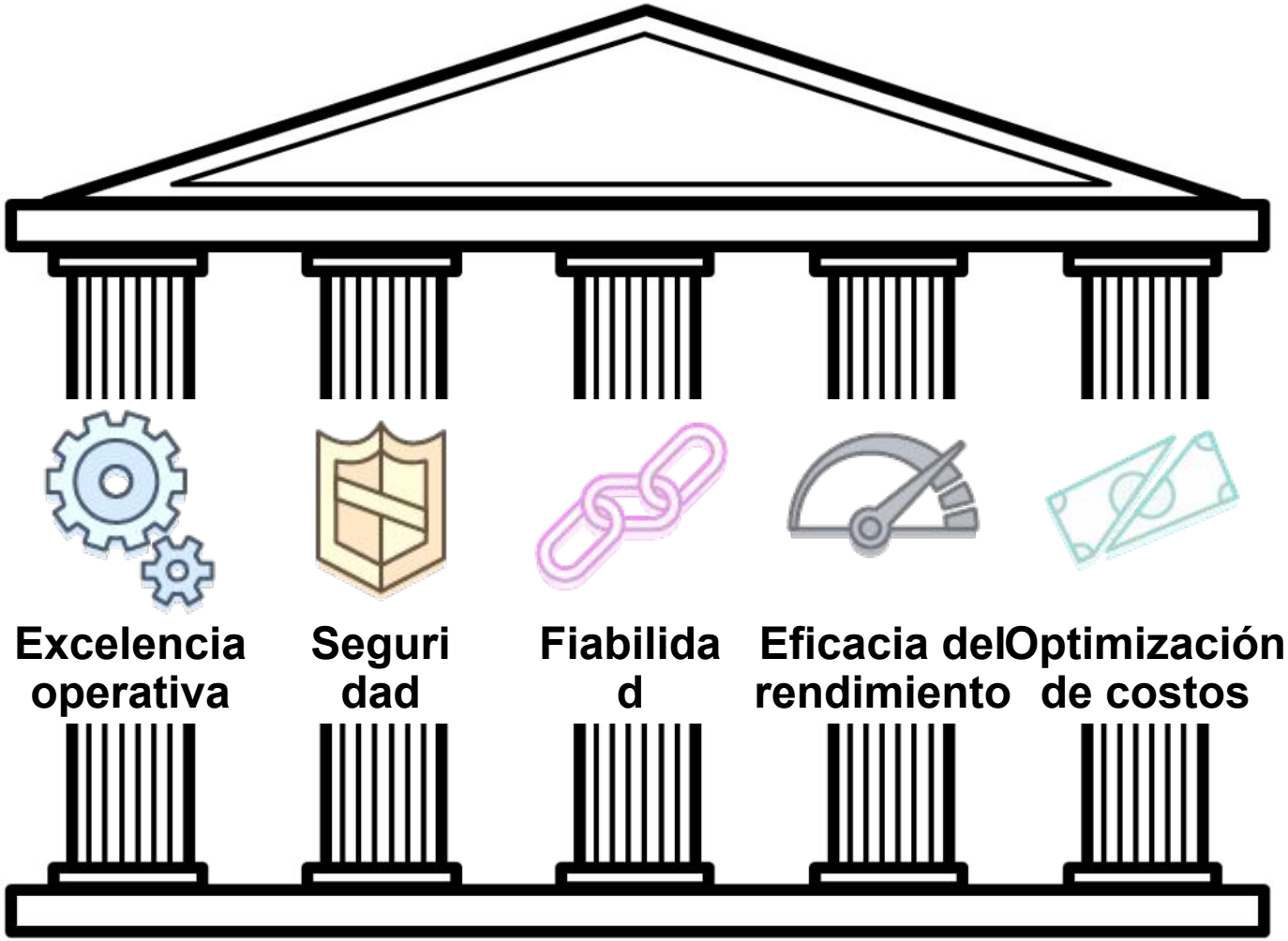
SEG. 1: ¿Cómo se administran las credenciales y la autenticación?

Los mecanismos de credenciales y autenticación incluyen contraseñas, tokens y claves que conceden acceso directa o indirectamente en su carga de trabajo. Proteja las credenciales con los mecanismos adecuados para ayudar a reducir el riesgo de uso accidental o malintencionado.

Prácticas recomendadas:

- Definir los requisitos para la administración de identidades y accesos
- Proteger al usuario raíz de la cuenta de AWS
- Exigir el uso de la autenticación multifactor
- Automatizar el cumplimiento de los controles de acceso
- Integrarse con un proveedor de federación centralizada
- Exigir los requisitos para contraseñas
- Rotar las credenciales con regularidad
- Auditar las credenciales de forma periódica

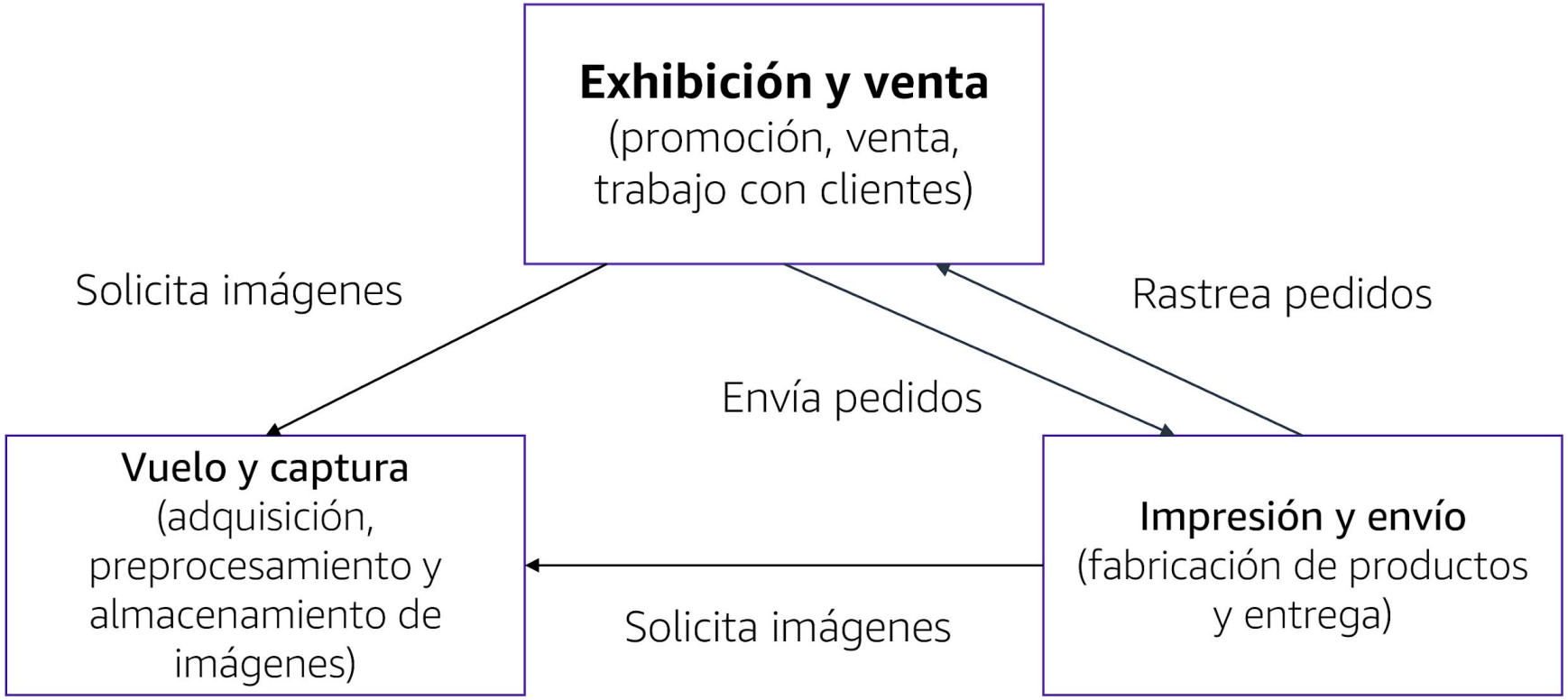
Introducción a la actividad “Principios de diseño del Marco de Buena Arquitectura de AWS”



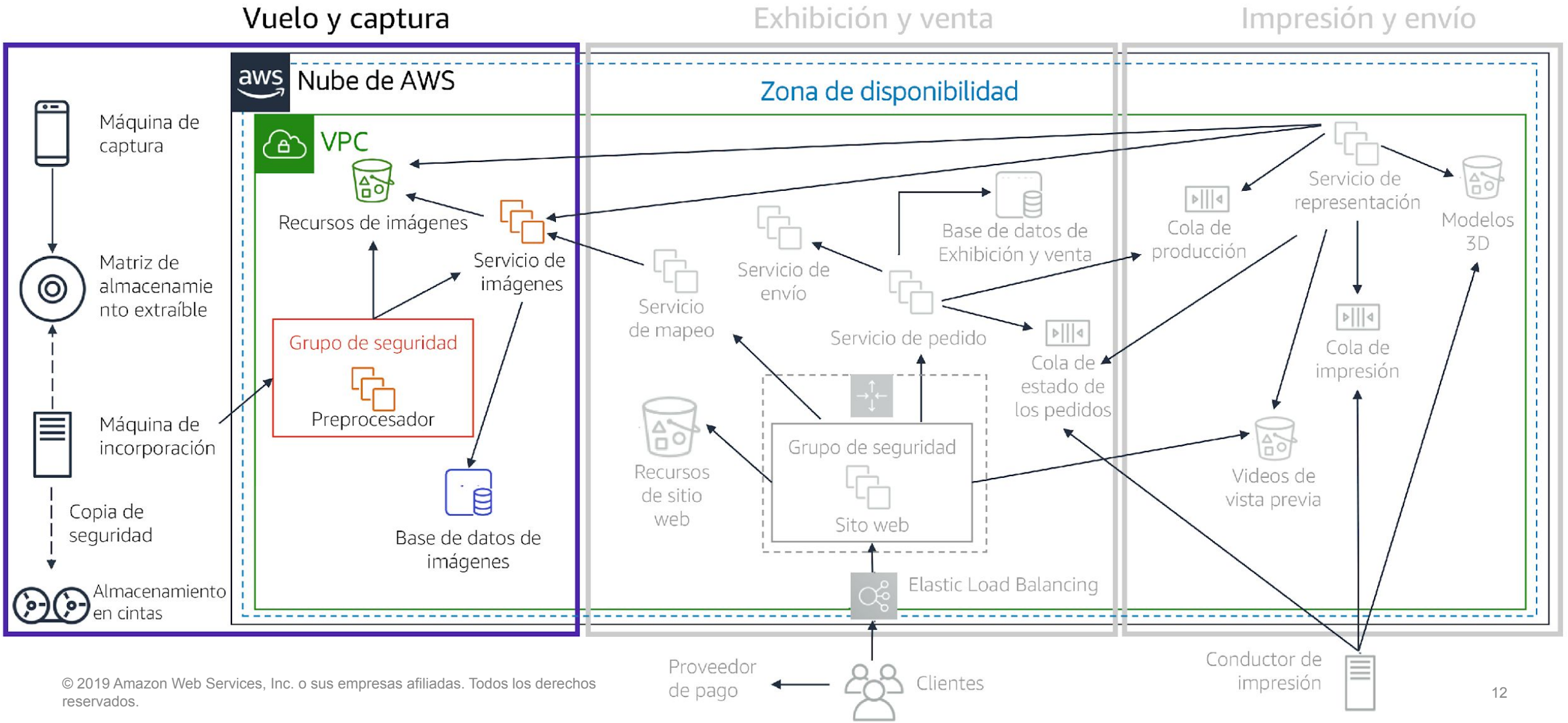
Información general sobre Empresa X

- Empresa X: "*Paisajes urbanos que puede ver como si estuviera volando*"
- Juan Pérez la fundó en el año 2008
- Vende paisajes urbanos impresos en 3D
- Está a punto de solicitar inversión
- **Le solicitó** que realizara una revisión de su plataforma como parte de su debida diligencia
- Nativa en la nube

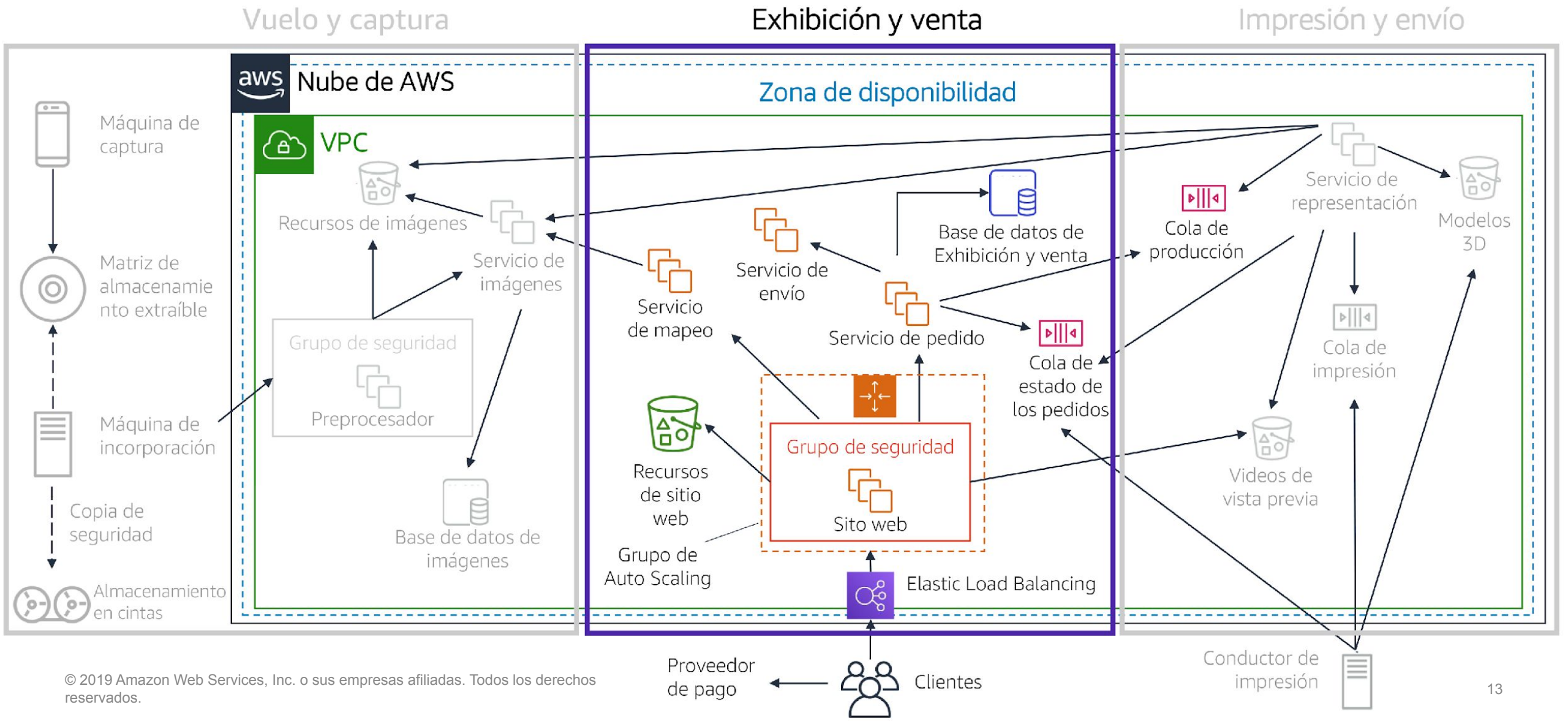
Información general sobre Empresa X (continuación)



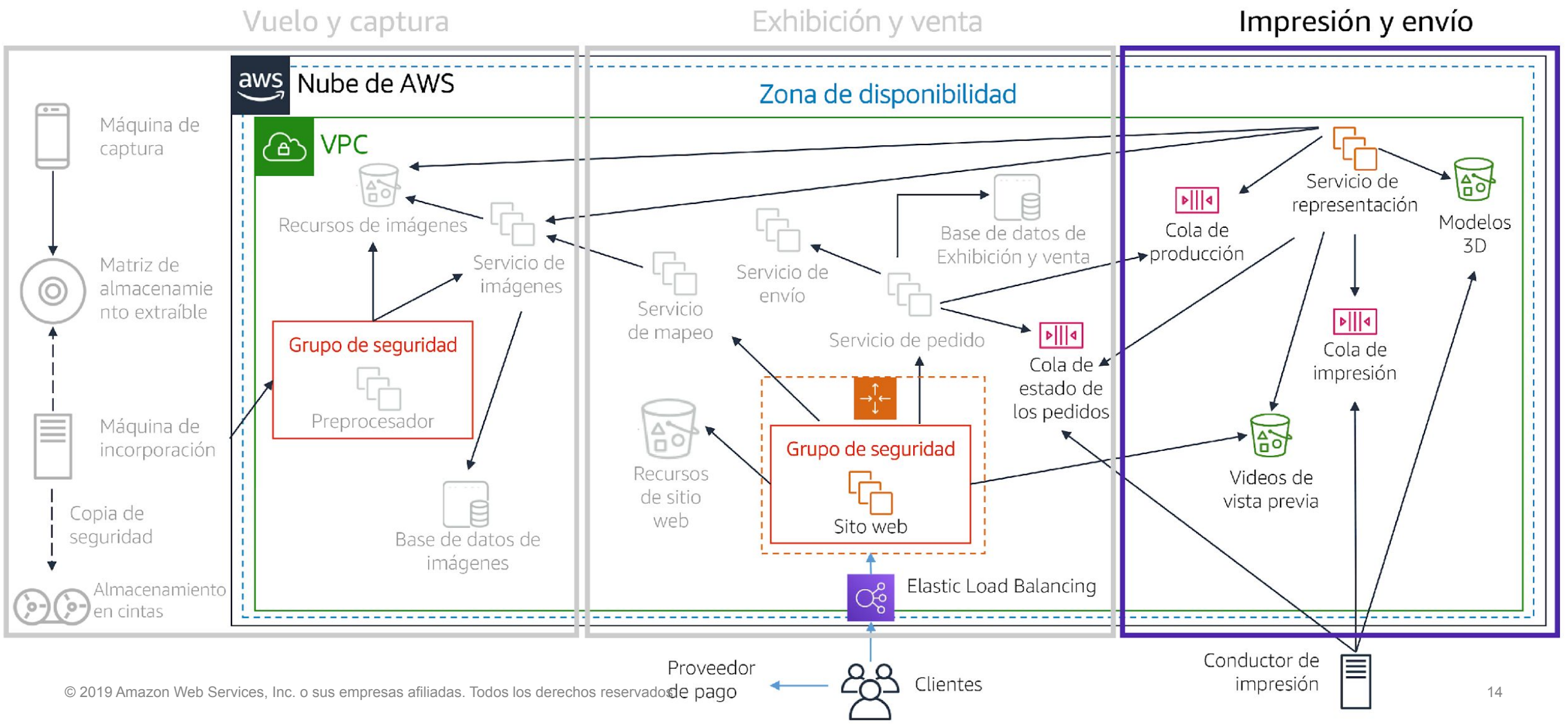
Arquitectura de Empresa X: vuelo y captura



Arquitectura de Empresa X: exhibición y venta



Arquitectura de Empresa X: impresión y envío



Información general sobre la actividad

- Deben formarse grupos pequeños.
- Aprenderá acerca de cada uno de los pilares. Después de revisar cada pilar, hay un conjunto de preguntas del Marco de Buena Arquitectura de AWS para que las analice con su grupo. Utilice estas preguntas del marco como guía para la revisión de la arquitectura de Empresa X.
- Respecto de cada pregunta del Marco de Buena Arquitectura, debe responder a las siguientes preguntas acerca de la arquitectura de Empresa X:
  - ¿Cuál es el ESTADO ACTUAL (qué hace Empresa X en la actualidad)?
  - ¿Cuál es el ESTADO FUTURO (qué cree que debería hacer Empresa X)?
- Determine con su grupo cuál es la mejora principal que Empresa X debe realizar en su arquitectura para cada conjunto de preguntas del Marco de Buena Arquitectura.
- Pista: no hay respuestas correctas ni incorrectas.

Pilar de excelencia operativa

Pilar de excelencia operativa

Pilar de excelencia operativa

Aporte valor de negocio.

- Enfoque
  - Ejecute y monitorice los sistemas con el objetivo de ofrecer valor de negocio, y mejore de forma continua los procesos y los procedimientos auxiliares.
- Temas clave
  - Administración y automatización de los cambios
  - Respuesta a eventos
  - Definición de estándares para administrar correctamente las operaciones diarias

Principios de diseño para la excelencia operativa

Pilar de excelencia operativa

Aporte valor de negocio.

- Realizar operaciones como código
- Comentar sobre la documentación
- Realizar cambios frecuentes, pequeños y reversibles
- Refinar los procedimientos de las operaciones con frecuencia
- Prever errores
- Aprender de todos los errores y los eventos operativos

Preguntas sobre la excelencia operativa

Preparación

- ¿Cómo se determinan las prioridades?
- ¿Cómo se diseña la carga de trabajo para poder comprender su estado?
- ¿Cómo se reducen los defectos, se facilita la reparación y se mejora el flujo hacia la producción?
- ¿Cómo se mitigan los riesgos de implementación?
- ¿Cómo se puede saber si se está preparado para admitir una carga de trabajo?

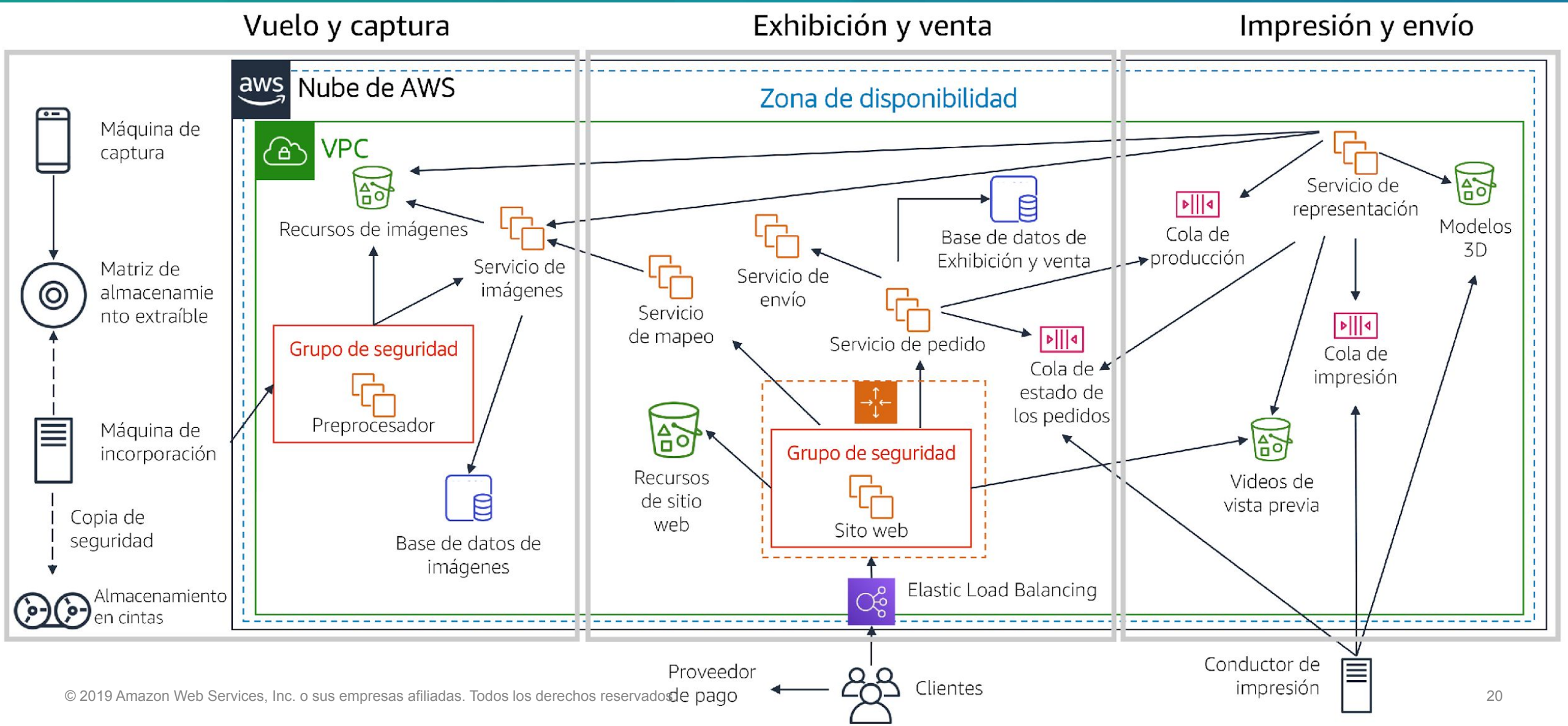
Operación

- ¿Cómo se entiende el estado de la carga de trabajo?
- ¿Cómo se entiende el estado de las operaciones?
- ¿Cómo se administran los eventos de las cargas de trabajo y las operaciones?

Evolución

- ¿Cómo se contribuye a la evolución de las operaciones?

Desglose de la actividad



Pilar de seguridad

Pilar de seguridad

Pilar de seguridad

Proteja y monitoree los sistemas.

- Enfoque
  - Proteja la información, los sistemas y los recursos, a la vez que aporta valor de negocio a través de evaluaciones de riesgo y estrategias de mitigación.
- Temas clave
  - Identificación y administración de quién puede hacer cada actividad
  - Configuración de controles para detectar eventos de seguridad
  - Protección de los sistemas y los servicios
  - Protección de la confidencialidad y la integridad de los datos

Principios de diseño para la seguridad

Pilar de seguridad

Proteja y monitoree los sistemas.

- Implementar una base sólida de identidades
- Habilitar la trazabilidad
- Aplicar la seguridad en todas las capas
- Automatizar las prácticas recomendadas de seguridad
- Proteger los datos en tránsito y en reposo
- Mantener a las personas alejadas de los datos
- Prepararse para eventos de seguridad

Preguntas sobre la seguridad

Administración de identidades y accesos

- ¿Cómo se administran las credenciales y la autenticación?
- ¿Cómo se controla el acceso humano?
- ¿Cómo se controla el acceso mediante programación?

Controles de detección

- ¿Cómo se detectan e investigan los eventos de seguridad?
- ¿Cómo se defiende contra las amenazas de seguridad emergentes?

Protección de infraestructuras

- ¿Cómo se protegen las redes?
- ¿Cómo se protegen los recursos informáticos?

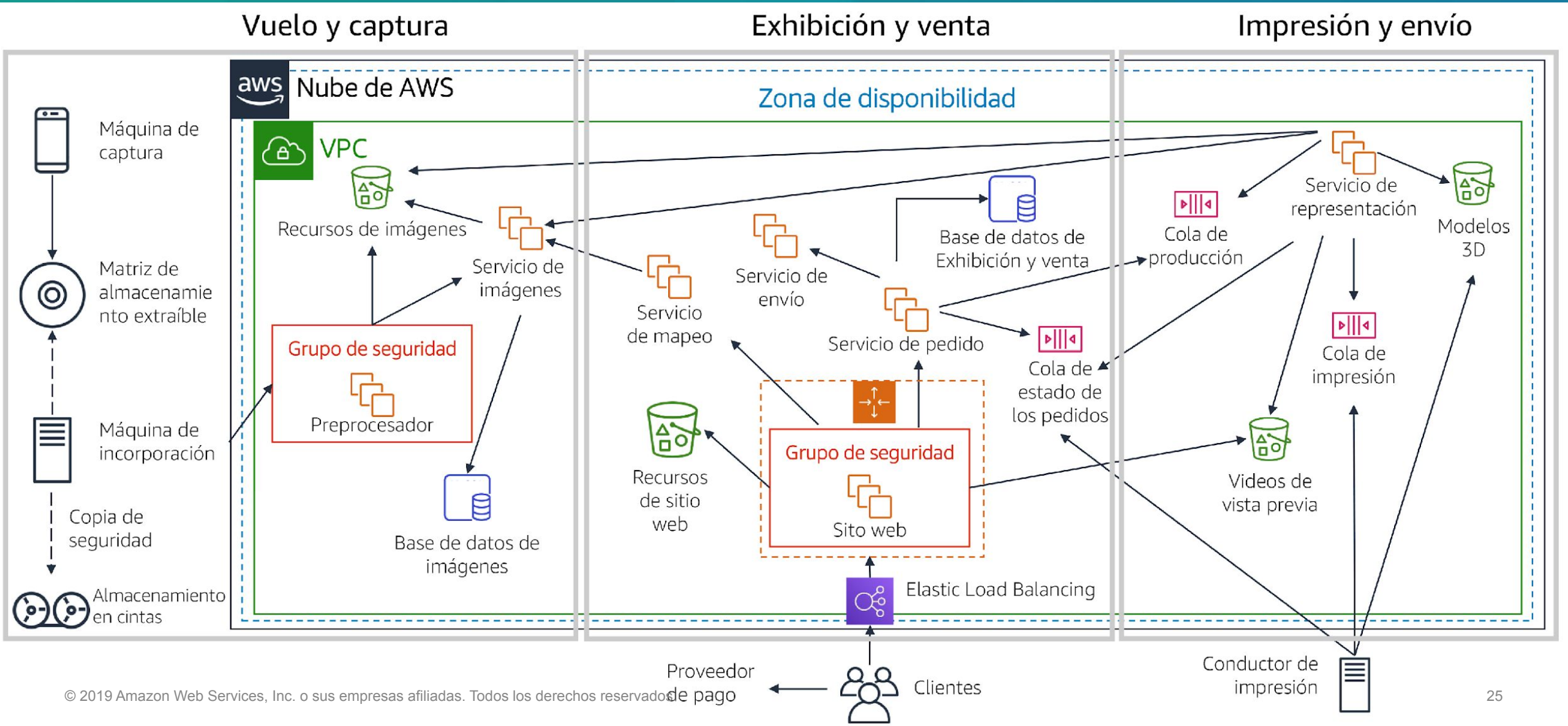
Protección de datos

- ¿Cómo se clasifican los datos?
- ¿Cómo se protegen los datos en reposo?
- ¿Cómo se protegen los datos en tránsito?

Respuesta a incidentes

- ¿Cómo se responde a un incidente?

Desglose de la actividad



Pilar de fiabilidad

Pilar de fiabilidad

Pilar de fiabilidad

Recupérese de los errores y mitigue las interrupciones

- Enfoque
  - Evite los errores y recupérese rápidamente después de que se produzcan para satisfacer la demanda del negocio y de los clientes.
- Temas clave
  - Configuración
  - Requisitos entre proyectos
  - Planificación de la recuperación
  - Gestión de cambios

Principios de diseño para la fiabilidad

Pilar de fiabilidad

Recupérese de los errores y mitigue las interrupciones

- Probar los procedimientos de recuperación
- Recuperarse automáticamente de los errores
- Escalar de manera horizontal para aumentar la disponibilidad total del sistema
- Evitar asumir estimaciones sobre capacidad
- Administrar los cambios en la automatización

Preguntas sobre la fiabilidad

Conceptos básicos

- ¿Cómo se administran los límites del servicio?
- ¿Cómo se administra la topología de red?

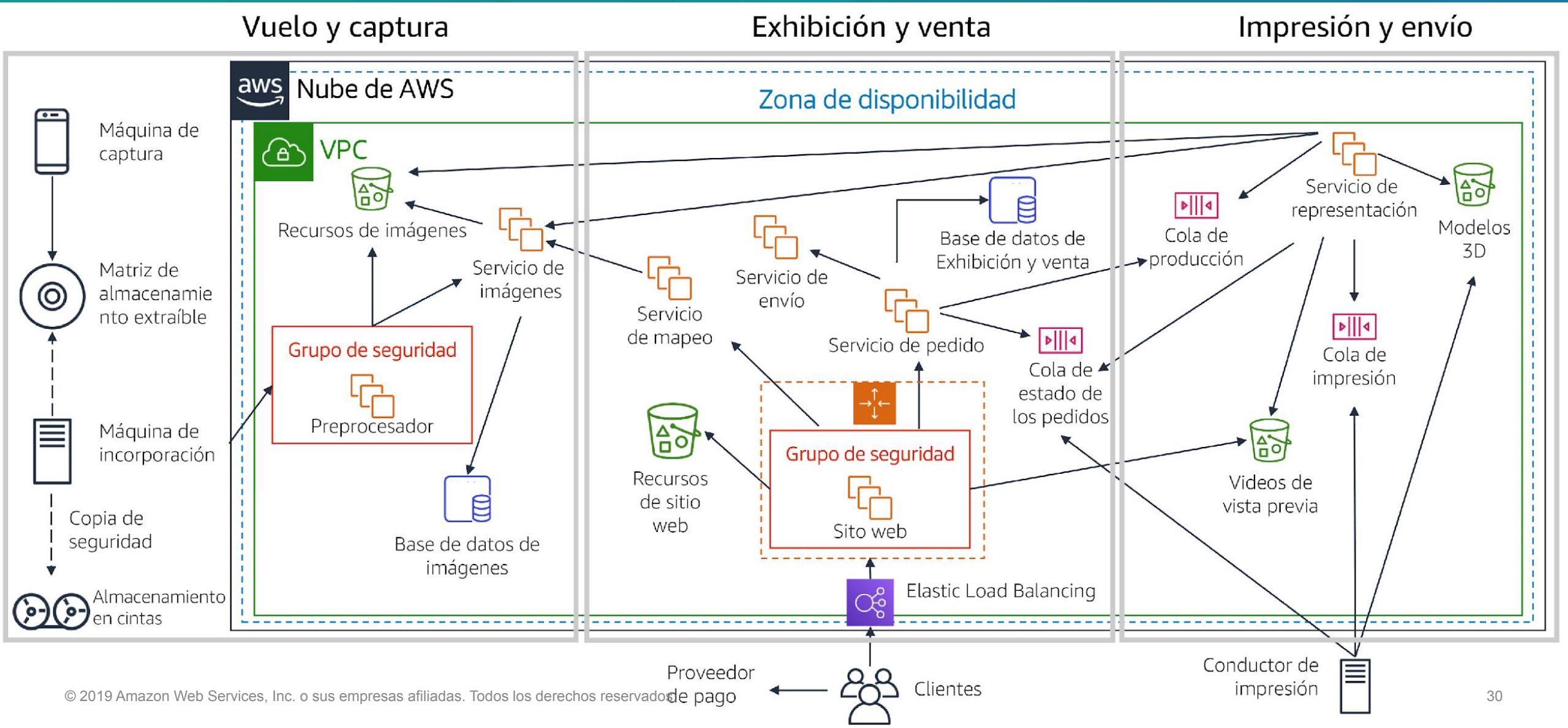
Administración de cambios

- ¿Cómo se adapta el sistema a los cambios en la demanda?
- ¿Cómo se monitorean los recursos?
- ¿Cómo se implementan los cambios?

Administración de errores

- ¿Cómo se generan copias de seguridad de los datos?
- ¿Cómo afronta el sistema los errores de los componentes?
- ¿Cómo se prueba la resiliencia?
- ¿Cómo se planifica la recuperación de desastres?

Desglose de la actividad



Pilar de eficacia del rendimiento

Pilar de eficacia del rendimiento

Pilar de eficacia del rendimiento

Utilice los recursos solo cuando sean necesarios.

- Enfoque
  - Utilice la TI y los recursos informáticos de forma eficaz para cumplir los requisitos del sistema y mantener esta eficacia a medida que cambia la demanda y evolucionan las tecnologías.
- Temas clave
  - Selección de los tipos y los tamaños adecuados de los recursos en función de los requisitos de la carga de trabajo
  - Monitoreo del rendimiento
  - Toma de decisiones fundamentadas para mantener la eficacia a medida que evolucionan las necesidades del negocio

Principios de diseño para la eficacia del rendimiento

Pilar de eficacia del rendimiento

Utilice los recursos solo cuando sean necesarios.

- Democratizar las tecnologías avanzadas
- Adquirir escala mundial en cuestión de minutos
- Utilizar arquitecturas sin servidor
- Experimentar más a menudo
- Disponer de compatibilidad mecánica

Preguntas sobre la eficacia del rendimiento

Selección

- ¿Cómo se selecciona la arquitectura con mejor rendimiento?
- ¿Cómo se selecciona la solución informática?
- ¿Cómo se selecciona la solución de almacenamiento?
- ¿Cómo se selecciona la solución de base de datos?
- ¿Cómo se selecciona la solución de red?

Revisión

- ¿Cómo se mejora la carga de trabajo para aprovechar las nuevas versiones?

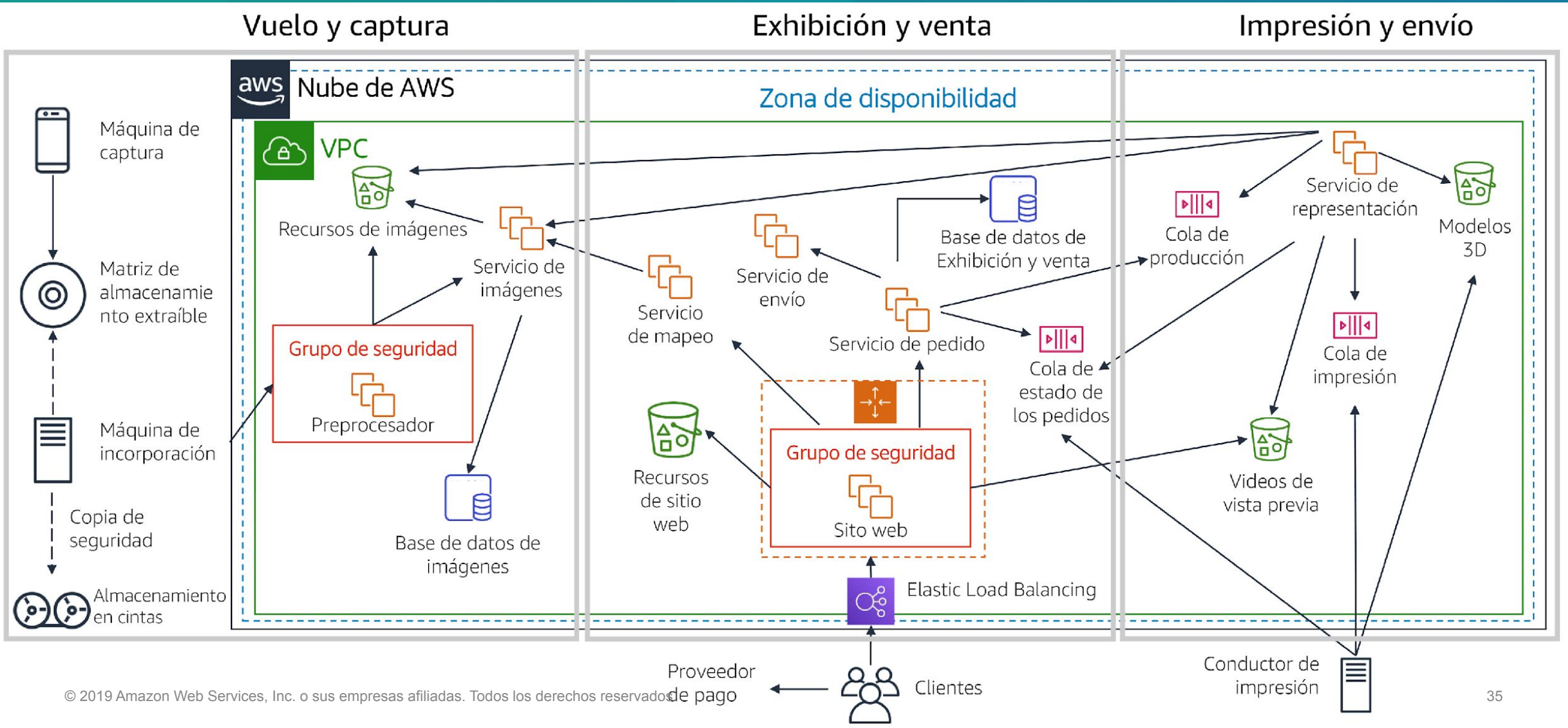
Monitoreo

- ¿Cómo se monitorean los recursos para asegurarse de que funcionen según lo previsto?

Compensaciones

- ¿Cómo se utilizan las compensaciones para mejorar el rendimiento?

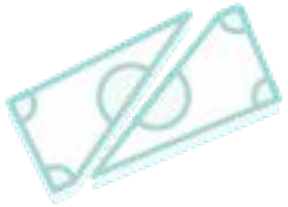
Desglose de la actividad



Pilar de optimización de costos

Pilar de optimización de costos

Pilar de optimización de costos

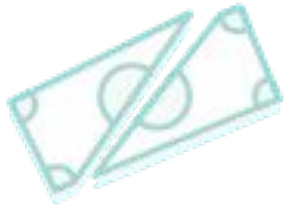


Elimine los gastos innecesarios

- Enfoque
  - Ejecute sistemas para aportar valor de negocio al menor precio.
- Temas clave
  - Conocimiento y control sobre los gastos
  - Selección de la cantidad más adecuada de tipos de recursos
  - Análisis de los gastos a lo largo del tiempo
  - Escalado para satisfacer las necesidades del negocio sin gastos excesivos

Principios de diseño para la optimización de costos

Pilar de optimización de costos



Elimine los gastos innecesarios

- Adoptar un modelo de consumo
- Medir la eficacia general
- Dejar de gastar dinero en las operaciones de centros de datos
- Analizar y atribuir los gastos
- Utilizar servicios administrados del nivel de aplicación para reducir el costo de propiedad

Preguntas sobre la optimización de costos

Conciencia del gasto

- ¿Cómo se controla el uso?
- ¿Cómo se monitorea el uso y el costo?
- ¿Cómo se retiran recursos?

Recursos rentables

- ¿Cómo se evalúa el costo cuando se seleccionan los servicios?
- ¿Cómo se cumplen los objetivos de costos cuando se selecciona el tipo y el tamaño de los recursos?
- ¿Cómo se utilizan los modelos de precios para reducir los costos?
- ¿Cómo se planifican los cambios en la transferencia de datos?

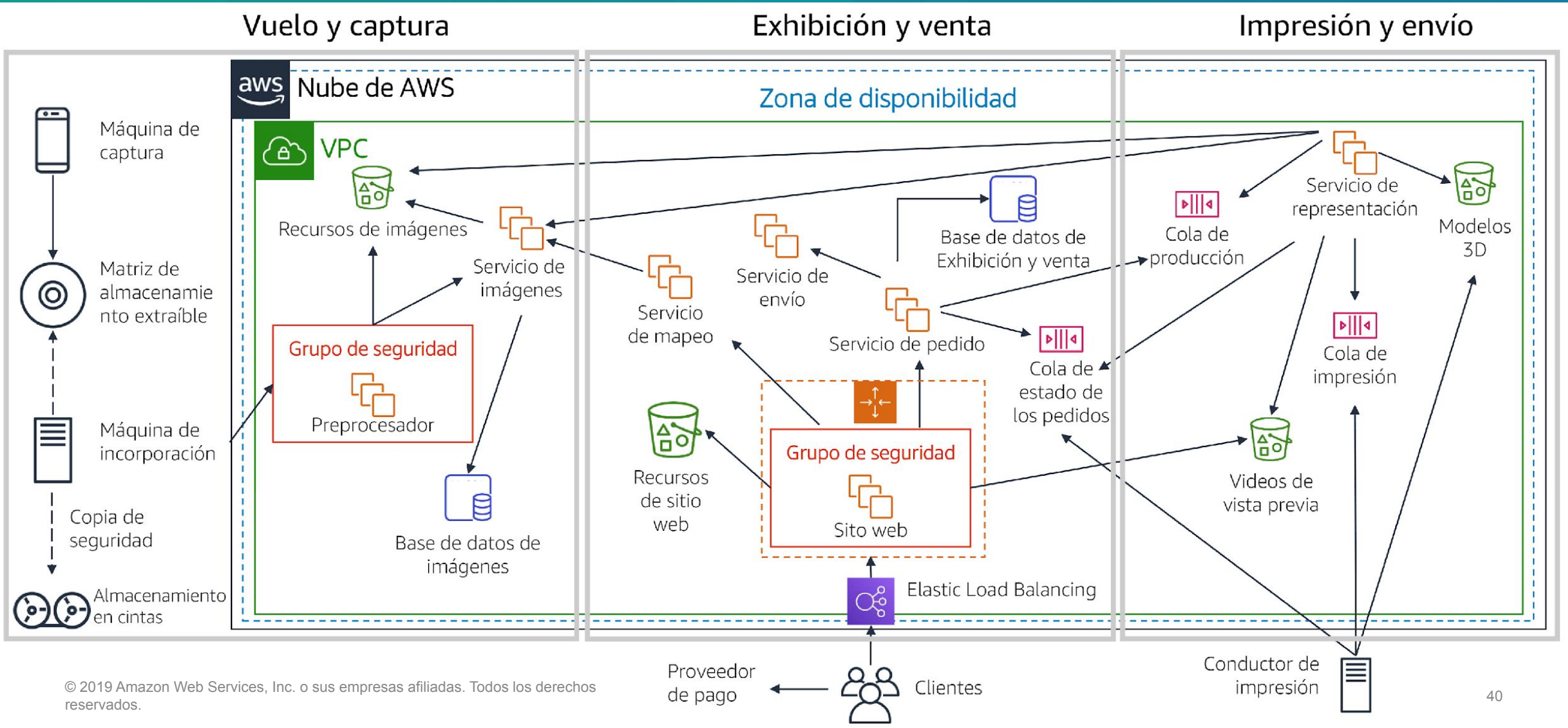
Ajuste entre la oferta y la demanda

- ¿Cómo se ajusta la oferta de recursos a la demanda?

Optimización a lo largo del tiempo

- ¿Cómo se evalúan los servicios nuevos?

Desglose de la actividad



AWS Well-Architected Tool

- Ayuda a revisar el estado de las cargas de trabajo y las compara con las prácticas recomendadas sobre arquitectura de AWS más recientes.
- Brinda acceso a los conocimientos y a las prácticas recomendadas que utilizan los arquitectos de AWS, siempre que necesite estos recursos.
- Ofrece un plan de acción con instrucciones paso a paso sobre cómo crear mejores cargas de trabajo para la nube.
- Ofrece un proceso uniforme para revisar y medir las arquitecturas en la nube.

Aprendizajes clave de la sección 1

- El Marco de Buena Arquitectura de AWS proporciona un enfoque uniforme para evaluar arquitecturas en la nube e instrucciones para ayudarlo a implementar diseños.
- El Marco de Buena Arquitectura de AWS documenta una serie de preguntas básicas que le permiten comprender si una arquitectura determinada se adecua a las prácticas recomendadas de la nube.
- El Marco de Buena Arquitectura de AWS se organiza en cinco pilares.
- Cada pilar incluye un conjunto de prácticas recomendadas y principios de diseño.

Módulo 9: Arquitectura en la nube

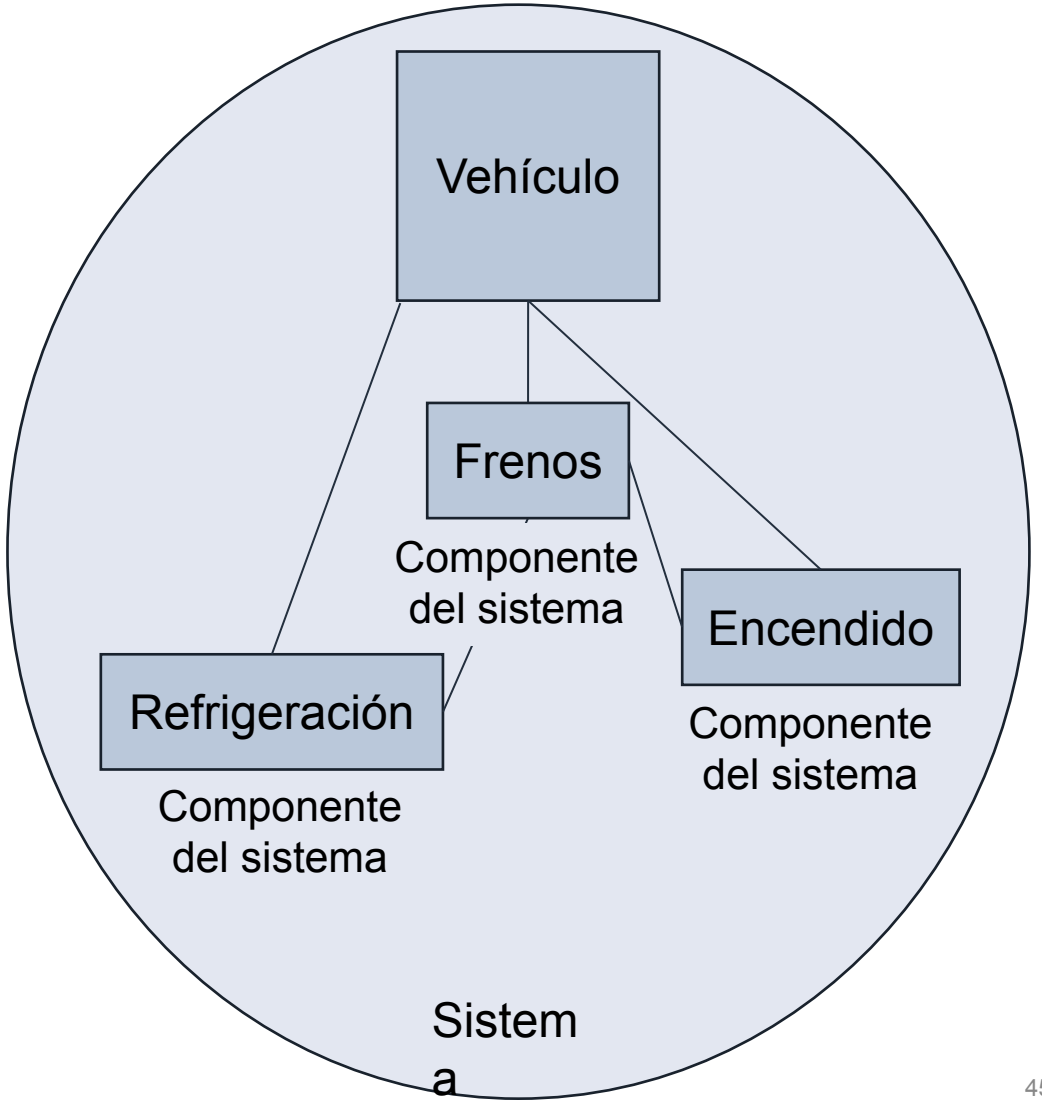
Sección 2: Fiabilidad y disponibilidad

“Todo falla constantemente”.

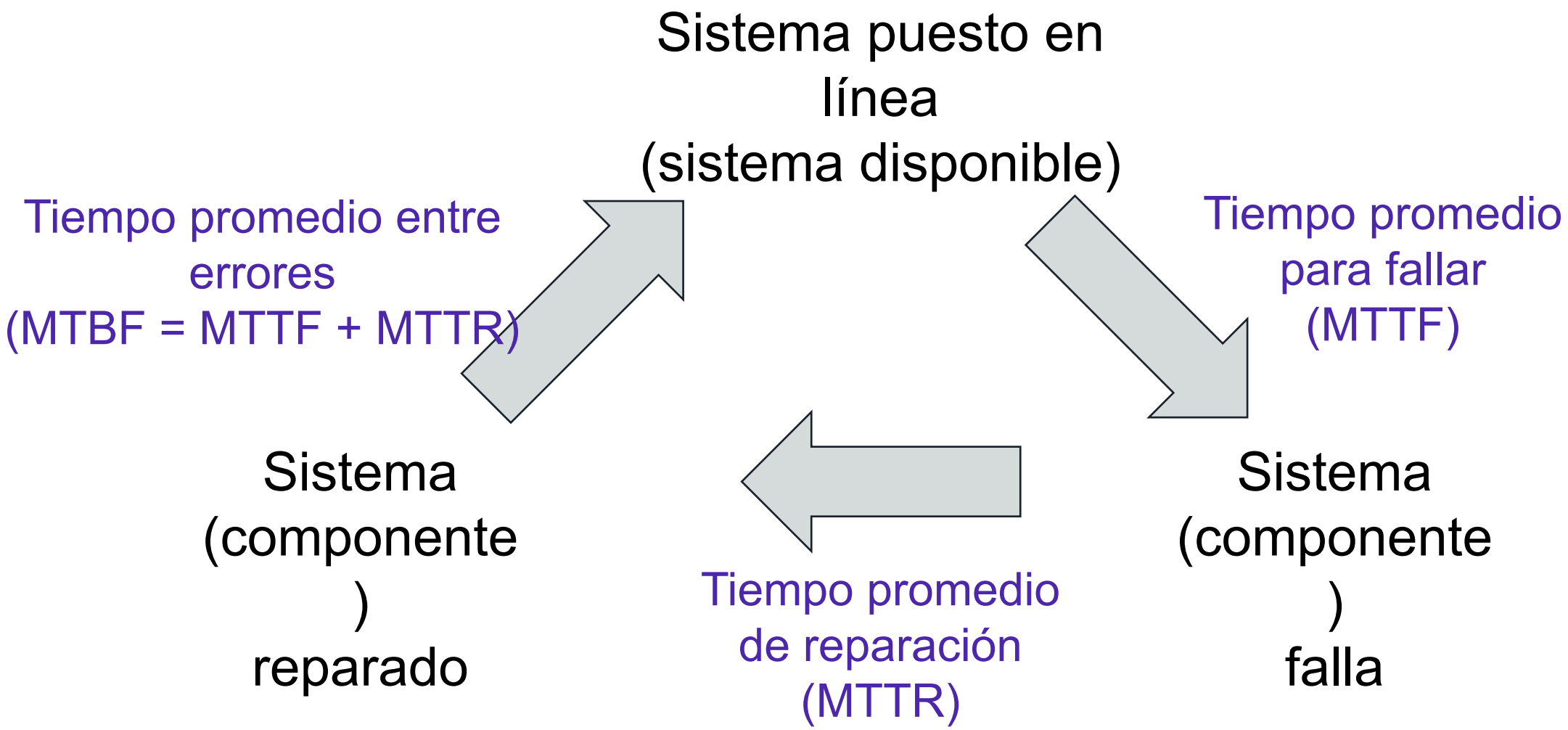
Werner Vogels, director de tecnología de Amazon.com

Fiabilidad

- Es una forma de medir la capacidad del sistema para proporcionar funcionalidad cuando lo desee el usuario.
- El sistema incluye todos los componentes de sistema:
  hardware, firmware y software.
- Es la probabilidad de que todo el sistema funcione según lo previsto durante un periodo especificado.
- Tiempo promedio entre errores (MTBF) = tiempo total en servicio/cantidad de errores



Comprensión de las métricas de fiabilidad



Disponibilidad

- Tiempo normal de operación/tiempo total
- Un porcentaje de tiempo de actividad (por ejemplo, 99,9 %) a lo largo del tiempo (por ejemplo, 1 año)
- Cantidad de números 9: cinco 9 implica una disponibilidad del 99,999 %

Alta disponibilidad

- El sistema puede resistir cierta medida de degradación sin dejar de estar disponible.
- Se minimiza el tiempo de inactividad.
- Se minimiza la intervención humana.

Capas de disponibilidad

Disponibilidad	Disrupción máxima (al año)	Categoría de aplicación
99 %	3 días, 15 horas	Trabajos de procesamiento por lotes, extracción, transferencia y carga de datos
99,9 %	8 horas, 45 minutos	Herramientas internas, como administración de conocimientos, seguimiento de proyectos
99,95 %	4 horas, 22 minutos	Comercio en línea, punto de venta
99,99 %	52 minutos	Sistemas de transmisión y entrega de videos
99,999 %	5 minutos	Transacciones de cajero automático, sistemas de telecomunicaciones

Factores que influyen en la disponibilidad

Tolerancia a errores

- La redundancia integrada de los componentes de una aplicación y su capacidad para permanecer operativos

Escalabilidad

- La habilidad de una aplicación para adaptarse a los aumentos en las necesidades de capacidad sin cambiar el diseño

Capacidad de recuperación

- Los procesos, las políticas y los procedimientos que están relacionados con el restablecimiento del servicio tras un evento catastrófico

Aprendizajes clave de la sección 2

- La fiabilidad es una medida de la capacidad del sistema para proporcionar funcionalidad cuando lo desee el usuario y se puede medir en términos de MTBF.
- La disponibilidad es el porcentaje de tiempo durante el cual un sistema funciona normal o correctamente realizando las operaciones que se esperan de él (o el tiempo de funcionamiento normal sobre el tiempo total).
- Tres factores que influyen en la disponibilidad de sus aplicaciones son la tolerancia a errores, la escalabilidad y la capacidad de recuperación.
- Puede diseñar sus cargas de trabajo y aplicaciones para que tengan alta disponibilidad, pero hay que tener en cuenta la compensación que esto implica para los costos.

Módulo 9: Arquitectura en la nube

Sección 3: AWS Trusted Advisor

AWS Trusted Advisor

AWS Trusted Advisor

- Es una herramienta en línea que ofrece instrucciones en tiempo real para ayudarlo a aprovisionar recursos según las prácticas recomendadas de AWS.
- Examina todo el entorno de AWS y ofrece recomendaciones en tiempo real en cinco categorías.

Optimización de costos

0 9 0

7516,85 USD

Posible ahorro mensual

Rendimiento

3 7 0

Seguridad

2 4 11

Tolerancia a errores

0 15 5

Service Limits

37 0 1

Actividad: Interpretación de las recomendaciones de AWS Trusted Advisor

Actividad: recomendación n.º 1

MFA en la cuenta raíz

Descripción: se verifica la cuenta raíz y se advierte si Multi-Factor Authentication (MFA) no está habilitada. Para aumentar el nivel de seguridad, le recomendamos que proteja la cuenta con MFA, la cual requiere que un usuario escriba un código de autenticación exclusivo desde su hardware MFA o dispositivo virtual al momento de interactuar con la consola de AWS y los sitios web asociados.

Criterios de alerta: la MFA no está habilitada en la cuenta raíz.

Acción recomendada: inicie sesión en su cuenta raíz y active un dispositivo MFA.

Actividad: recomendación n.º 2

Política de contraseñas de IAM

Descripción: se verifica la política de contraseñas de la cuenta y se advierte cuando una política no está habilitada. También se indica si no se habilitaron los requisitos de contenido de la contraseña. Los requisitos de contenido de la contraseña aumentan el nivel de seguridad general del entorno de AWS al imponer
la creación de contraseñas de usuario seguras. Cuando se crea o se modifica una política de contraseñas, el cambio se aplica de forma inmediata a los usuarios nuevos. Sin embargo, no se obliga a los usuarios existentes a cambiar sus contraseñas.

Criterios de alerta: hay una política de contraseñas habilitada, pero al menos un requisito del contenido no está habilitado.

Acción recomendada: si algunos requisitos de contenido no están habilitados, considere su habilitación. Si no hay una política de contraseñas habilitada, cree y configure una. Consulte “Configuración de una política de contraseñas de la cuenta para usuarios de IAM”.

Actividad: recomendación n.º 3

Grupos de seguridad: acceso sin restricciones

Descripción: se verifican los grupos de seguridad para detectar reglas que permitan obtener acceso a un recurso sin restricciones. El acceso sin restricciones aumenta las posibilidades de que ocurra actividad maliciosa (jaqueos, ataques de denegación de servicio, pérdida de datos).

Criterios de alerta: la regla de un grupo de seguridad tiene una dirección IP de origen con un sufijo /0 para puertos distintos de 25, 80 o 443.

Acción recomendada: restrinja el acceso a solo aquellas direcciones IP que lo necesiten. Para limitar el acceso a una dirección IP específica, establezca el sufijo en /32 (por ejemplo, 192.0.2.10/32). Asegúrese de eliminar las reglas excesivamente permisivas después de crear reglas más restrictivas.

Región	Nombre del grupo de seguridad	ID del grupo de seguridad	Protocolo	Puerto	Estado	Intervalo de IP
us-east-1	WebServerSG	sg-xxxxxxx1 (vpc-xxxxxxx1)	tcp	22	Rojo	0.0.0.0/0
us-west-2	DatabaseServerSG	sg-xxxxxxx2 (vpc-xxxxxxx2)	tcp	8080	Rojo	0.0.0.0/0

Actividad: recomendación n.º 4

Instantáneas de Amazon EBS

Descripción: se verifica la antigüedad de las instantáneas de los volúmenes de Amazon Elastic Block Store (Amazon EBS), ya sea que estén disponibles o en uso. Aunque se repliquen los volúmenes de Amazon EBS, pueden producirse errores. Se crean instantáneas de manera continua en Amazon Simple Storage Service (Amazon S3) para lograr un almacenamiento duradero y para poder realizar recuperaciones a un momento dado.

Criterios de alerta:
Amarillo: la instantánea de volumen más reciente tiene entre 7 y 30 días de antigüedad.
Rojo: la instantánea de volumen más reciente tiene más de 30 días de antigüedad.
Rojo: el volumen no tiene ninguna instantánea.

Acción recomendada: cree instantáneas semanales o mensuales de sus volúmenes.

Región	ID del volumen	Nombre del volumen	ID de la instantánea	Nombre de la instantánea	Antigüedad de la instantánea	Asociación de volúmenes	Estado	Motivo
us-east-1	vol-xxxxxxxx	My-EBS-Volume				/dev/…	Rojo	Sin instantánea

Actividad: recomendación n.º 5

Registro de buckets de Amazon S3
Descripción: se verifica la configuración de registro de buckets de Amazon Simple Storage Service (Amazon S3). Cuando
se habilita el registro de acceso al servidor, se envían registros de acceso detallados una vez por hora a un bucket que usted elija. Un registro de acceso incluye información detallada sobre cada solicitud, como el tipo de solicitud, los recursos especificados en la solicitud y la hora y la fecha en la que se procesó. De manera predeterminada, el registro
de buckets no está habilitado. Debe habilitarlo si desea realizar auditorías de seguridad u obtener más información sobre los usuarios y los patrones de uso.
Criterios de alerta:
Amarillo: el bucket no tiene habilitado el registro de acceso al servidor.
Amarillo: los permisos del bucket de destino no incluyen la cuenta del propietario. Trusted Advisor no puede comprobarlo.
Acción recomendada:
Habilite el registro de buckets para la mayoría de ellos. Si los permisos del bucket de destino no incluyen la cuenta del
com

Región	Nombre del bucket	Nombre del destino	Existencia del destino	Mismo propietario	Escritura habilitada	Motivo
us-east-2	my-hello-world-bucket		No	No	No	Registro no habilitado

etario

Aprendizajes clave de la sección 3

- AWS Trusted Advisor es una herramienta en línea que suministra asesoramiento en tiempo real para ayudarlo a aprovisionar recursos según las prácticas recomendadas de AWS.
- AWS Trusted Advisor examina todo el entorno de AWS y le ofrece recomendaciones en tiempo real en cinco categorías.
- Puede utilizar AWS Trusted Advisor como ayuda para optimizar el entorno de AWS tan pronto como comience a implementar sus diseños de arquitectura.

Módulo 9: Arquitectura en la nube

Conclusión del módulo

Resumen del módulo

En resumen, en este módulo, aprendió a hacer lo siguiente:

- Describir el Marco de Buena Arquitectura de AWS, incluidos los cinco pilares
- Identificar los principios de diseño del Marco de Buena Arquitectura de AWS
- Explicar la importancia de la fiabilidad y la alta disponibilidad
- Identificar cómo AWS Trusted Advisor ayuda a los clientes
- Interpretar las recomendaciones de AWS Trusted Advisor

Complete la revisión de conocimientos

Pregunta del examen de muestra

Un ingeniero de SysOps que trabaja en una empresa quiere proteger sus datos en tránsito y en reposo. ¿Qué servicios podría utilizar para proteger los datos?

A. Elastic Load Balancing
B. Amazon Elastic Block Store (Amazon EBS)
C. Amazon Simple Storage Service (Amazon S3)
D. Todas las opciones anteriores

Recursos adicionales

- Sitio web del Marco de Buena Arquitectura de AWS
- Documento técnico del Marco de Buena Arquitectura de AWS
- Laboratorios de AWS Well-Architected
- Verificaciones de prácticas recomendadas de AWS Trusted Advisor

Gracias

aws academy