COLOMBIA POTENCIA DE LA VIDA

TIC

LECCIÓN 3: PATRONES DE RECUPERACIÓN DE DESASTRES

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

UTP Universidad Tecnológica de Pereira

PATRONES COMUNES DE RECUPERACIÓN DE DESASTRES EN AWS

CUATRO PATRONES DE RECUPERACIÓN DE DESASTRES

- **Copia de seguridad y restauración**
- **Luz piloto**
- **Espera semiactiva**
- **Sitios múltiples**

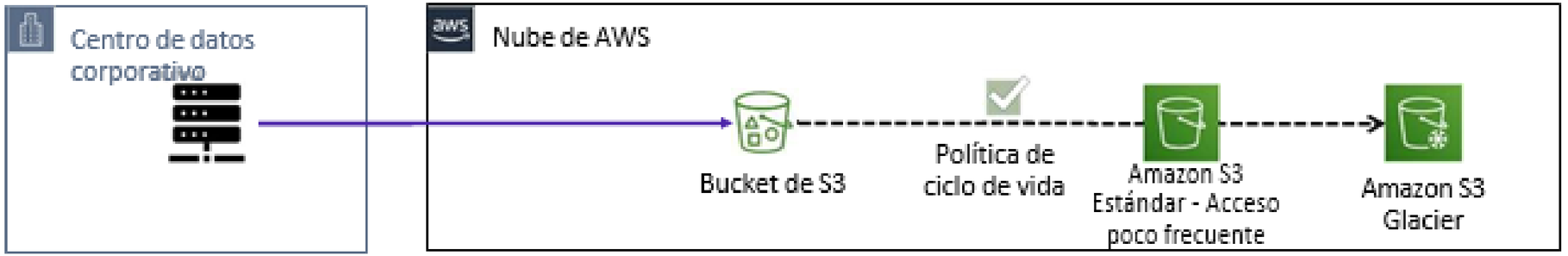
CADA PATRÓN ES ADECUADO PARA UNA COMBINACIÓN DIFERENTE DE LOS SIGUIENTES ELEMENTOS:

- **Objetivo de tiempo de recuperación**
- **Objetivo de punto de recuperación**
- **Rentabilidad**

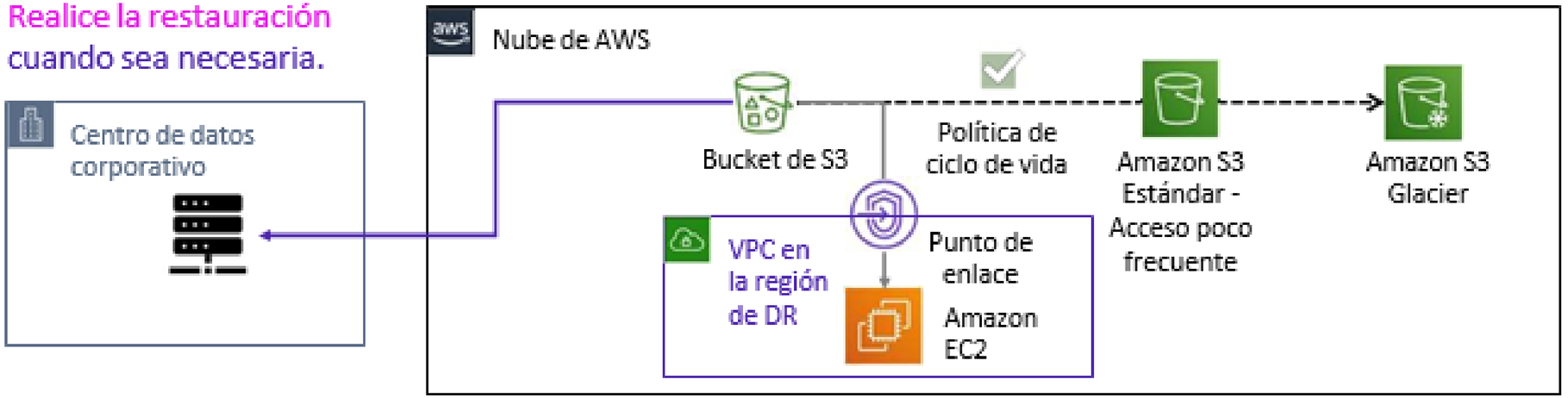
Como podrá ver en los siguientes detalles, cada patrón se adapta bien a diferentes requisitos. Algunos de los patrones ofrecen más rentabilidad. Otros proporcionan un RPO y un RTO más rápidos, pero cuesta más mantenerlos.

PATRÓN DE COPIA DE SEGURIDAD Y RESTAURACIÓN

Realice una copia de seguridad de los datos de configuración y estado en S3. Implemente una política de ciclo de vida para ahorrar costos.



Realice la restauración cuando sea necesaria.



El primer enfoque para la recuperación de desastres es el patrón de copia de seguridad y restauración.

En la mayoría de los entornos tradicionales, se realiza una copia de seguridad de los datos en cinta y se envían fuera del sitio con regularidad. Si utiliza este método, puede tardar mucho tiempo en restaurar el sistema cuando se produce un desastre.

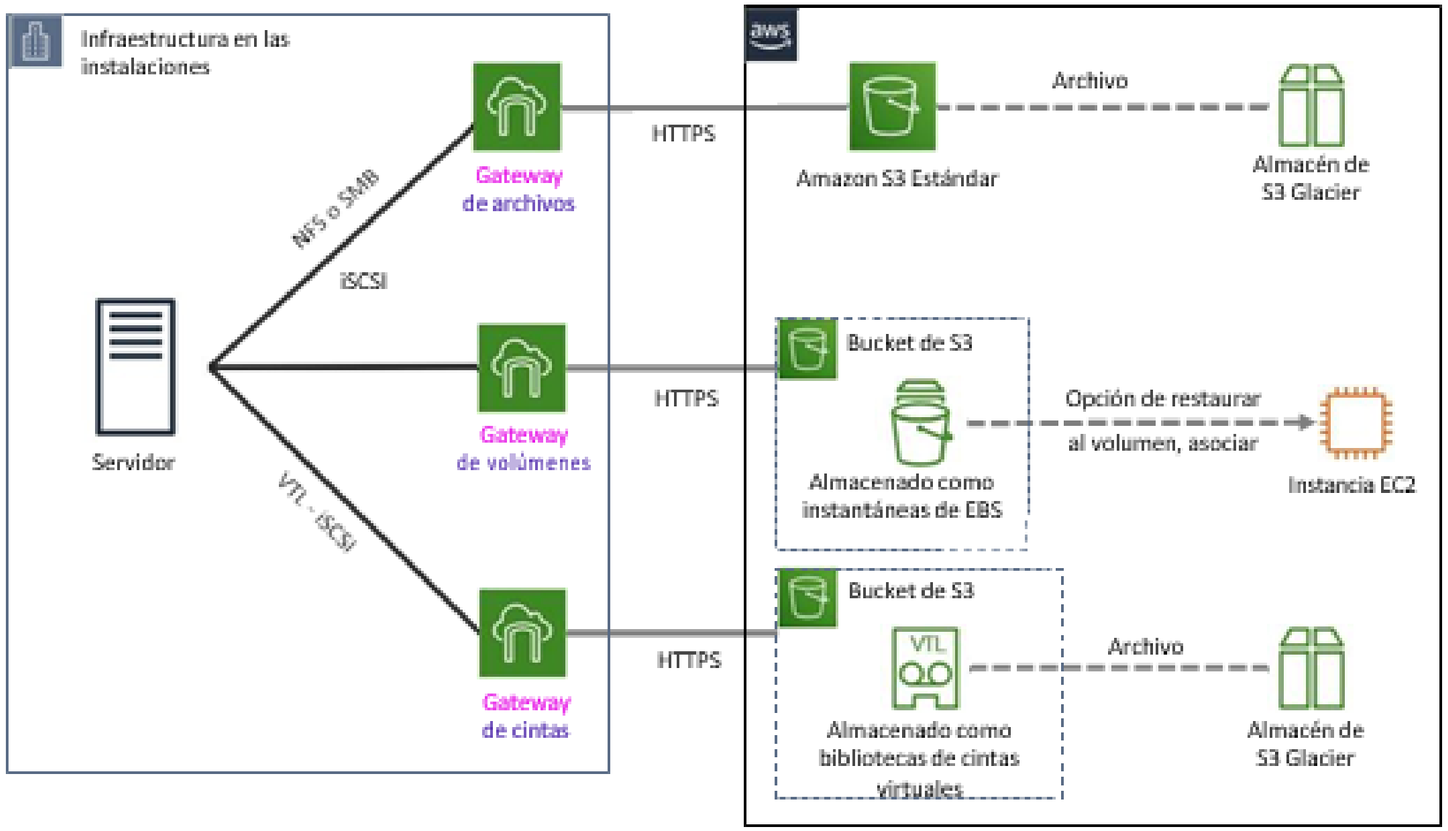
Amazon S3 proporciona un destino de acceso más fácil a los datos de copia de seguridad que podrían necesitarse rápidamente para realizar una restauración. La transferencia de datos hacia y desde Amazon S3 suele efectuarse a través de la red; por lo tanto, se puede acceder a ellos desde cualquier ubicación.

En el caso de copia de seguridad de ejemplo, los datos se copian del centro de datos en las instalaciones a Amazon S3. Puede usar AWS DataSync o Amazon S3 Transfer Acceleration como parte de esta configuración para automatizar o aumentar la velocidad de la transferencia de datos. Luego, una configuración del ciclo de vida de S3 que se aplica al bucket posteriormente traslada los datos de copia de seguridad a clases de almacenamiento de Amazon S3 menos costosas. Los datos de copia de seguridad se trasladan a Amazon S3 Glacier o Amazon S3 Estándar - Acceso poco frecuente, lo que ahorra costos a medida que los datos se vuelven obsoletos y no se accede a ellos con frecuencia.

En el caso de restauración de ejemplo, es posible que los datos en las instalaciones se pierdan de manera temporal o permanente. En ese caso, los datos de copia de seguridad se pueden descargar de Amazon S3 de nuevo en los servidores en las instalaciones.

Si el centro de datos corporativo se mantiene sin conexión, puede garantizar aún más la capacidad de restaurar los datos en sus servidores. Puede tener servidores de Amazon EC2 que estén listos para ingresar en una VPC de la región de recuperación de desastres designada. Esta región puede conectarse al bucket de S3 que contiene los datos de la aplicación de copia de seguridad. Puede leer esos datos y quizás alojar temporalmente las aplicaciones mientras trabaja para restaurar el centro de datos.

AWS STORAGE GATEWAY



Como parte del patrón de copia de seguridad y restauración, tal vez note que tiene sentido utilizar AWS Storage Gateway.

AWS Storage Gateway es un servicio de almacenamiento híbrido que permite a las aplicaciones en las instalaciones usar el almacenamiento en la nube de AWS. Puede utilizar el servicio para copia de seguridad y archivo, recuperación de desastres, procesamiento de datos en la nube, almacenamiento por niveles y migración.

Sus aplicaciones se conectan al servicio a través de una máquina virtual o un dispositivo hardware de gateway con protocolos de almacenamiento estándar. Estos protocolos incluyen NFS, SMB, biblioteca de cintas virtuales (VTL) e interfaz de sistema para equipos pequeños de Internet (iSCSI). La gateway se conecta a los servicios de almacenamiento de AWS, como Amazon S3, Amazon S3 Glacier y Amazon EBS, los cuales permiten almacenar archivos, volúmenes y cintas virtuales. El servicio incluye un mecanismo de transferencia de datos optimizado. Proporciona administración del ancho de banda, resiliencia de las redes automatizada y transferencia de datos eficiente, además de una caché local para lograr un acceso en las instalaciones de baja latencia a los datos más activos.

Con una gateway de archivos, almacena y recupera objetos (mediante el protocolo NFS o SMB) en Amazon S3. Utiliza una caché local para lograr un acceso de baja latencia a los datos utilizados más recientemente. Cuando los archivos se transfieren a Amazon S3, se almacenan como objetos y se puede acceder a ellos a través de un punto de montaje NFS.

La interfaz de volúmenes de Storage Gateway presenta las aplicaciones con volúmenes de discos de almacenamiento en bloque a los que se puede acceder con el protocolo iSCSI. A los datos de estos volúmenes se les realizan copias de seguridad con instantáneas de EBS a un momento dado, lo que le permite acceder a ellos a través de Amazon EC2, si resulta necesario.

La interfaz de cintas de Storage Gateway presenta la gateway de almacenamiento a su aplicación de copia de seguridad existente como una biblioteca de cintas virtuales. Esta biblioteca consta de un cambiador de medios virtual y unidades de cintas virtuales. Puede seguir utilizando las aplicaciones de copia de seguridad existentes mientras escribe en una colección de cintas virtuales. Cada cinta virtual se almacena en Amazon S3. Cuando ya no necesita acceder a los datos de las cintas virtuales, la aplicación de copia de seguridad los guarda desde la biblioteca de cintas virtuales en Amazon S3 Glacier.

COPIA DE SEGURIDAD Y RESTAURACIÓN: LISTA DE COMPROBACIÓN

FASE DE PREPARACIÓN

- **Realice copias de seguridad de los sistemas actuales**
- **Almacene las copias de seguridad en Amazon S3.**
- **Documente el procedimiento necesario para realizar la restauración a partir de copias de seguridad**
- **Debe saber lo siguiente:**

Qué AMI utilizar y crear según la necesidad

Cómo restaurar el sistema a partir de las copias de seguridad

Cómo dirigir el tráfico al nuevo sistema

Cómo configurar la implementación

EN CASO DE DESASTRE

- **Recupere las copias de seguridad de Amazon S3.**

- **Restaure la infraestructura necesaria.**

  - Instancias EC2 que surgen de AMI preparadas

  - Balanceadores de carga de Elastic Load Balancing

  - Recursos de AWS creados por una pila de AWS CloudFormation: implementación automatizada para restaurar o duplicar el entorno

- **Restaure el sistema a partir de una copia de seguridad.**

- **Dirija el tráfico al nuevo sistema.**

  - Ajuste los registros del sistema de nombres de dominio (DNS) como corresponda.

COLOMBIA POTENCIA DE LA VIDA

TIC

Si implementa el patrón de recuperación de desastres de copia de seguridad y restauración, los pasos clave que debe completar durante la fase de preparación son los siguientes:

- Realice copias de seguridad de los sistemas actuales.
- Almacene las copias de seguridad en Amazon S3.
- Documente el procedimiento de restauración a partir de copias de seguridad.

Si implementa este patrón, los pasos clave que debe completar si ocurre un desastre son los siguientes:

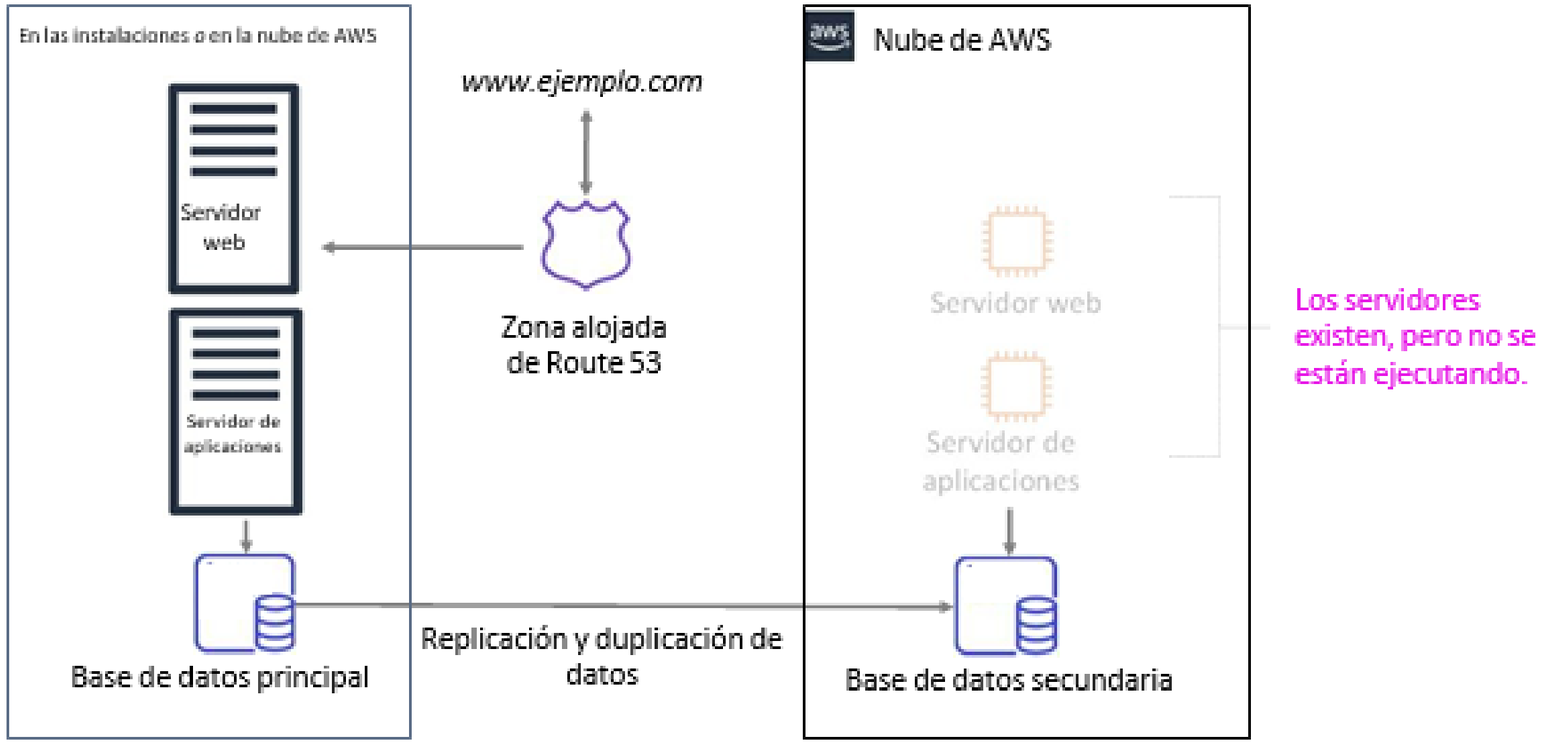
- Recupere las copias de seguridad de Amazon S3.
- Inicie la infraestructura requerida.
- Restaure el sistema a partir de las copias de seguridad.
- Por último, dirija el tráfico al nuevo sistema.

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

UTP Universidad Tecnológica de Pereira

PATRÓN DE LUZ PILOTO: FASE DE PREPARACIÓN



El segundo enfoque de recuperación de desastres es el patrón de luz piloto.

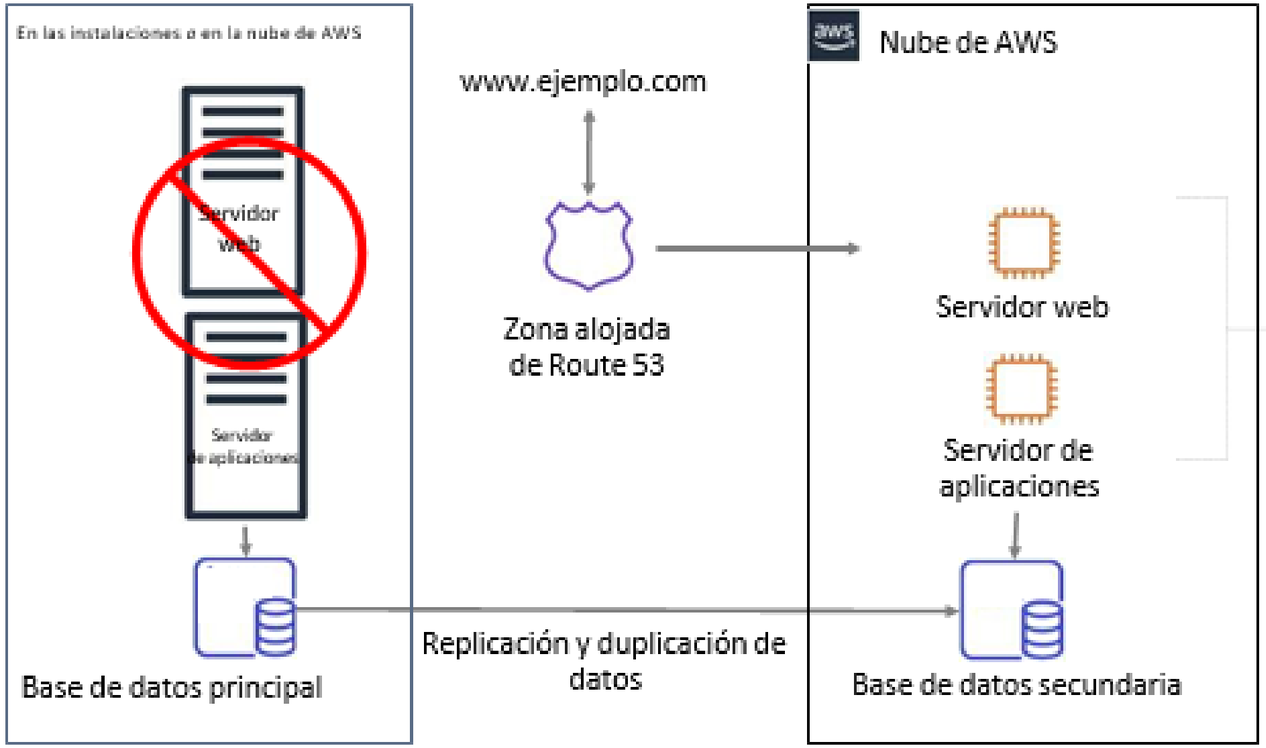
Luz piloto describe un patrón de recuperación de desastres en el que una versión mínima de copia de seguridad de su entorno siempre se está ejecutando. La analogía de la luz piloto proviene de un calentador de gas: una llama pequeña (o la luz piloto) siempre está encendida, incluso cuando el calentador está apagado. La luz piloto puede encender rápidamente toda la caldera para calentar una casa. En el patrón de ejemplo, la luz piloto es la base de datos secundaria que siempre está en ejecución.

El caso de luz piloto es similar a la de copia de seguridad y restauración. Sin embargo, la recuperación suele ser más corta porque las piezas principales del sistema ya se están ejecutando y se mantienen continuamente actualizadas. Cuando llega el momento de la recuperación, puede aprovisionar con rapidez un entorno de producción completo alrededor del núcleo crítico.

Los elementos de infraestructura correspondientes a la luz piloto en sí suelen incluir los servidores de base de datos. Esta agrupación es el núcleo crítico del sistema (la luz piloto). Todas las demás piezas de infraestructura se pueden aprovisionar rápidamente alrededor del núcleo para restaurar todo el sistema. Para aprovisionar el resto de la infraestructura, normalmente se agrupan servidores configurados con anterioridad como AMI que están listas para iniciarse de inmediato. (O pueden ser instancias en estado detenido). Cuando comienza la recuperación, estas instancias inician de manera rápida con su rol predefinido, lo que les permite conectarse a la base de datos.

Implementar este patrón es relativamente económico. Los datos que cambian con regularidad deben replicarse con luz piloto, el núcleo pequeño para el cual se iniciará el entorno completo en la fase de recuperación. Los datos actualizados con menos frecuencia, como los sistemas operativos y las aplicaciones, se pueden actualizar de manera periódica y almacenar como AMI.

PATRÓN DE LUZ PILOTO: EN CASO DE DESASTRE



Los servidores empiezan a funcionar en pocos minutos.

Supongamos que ocurre un desastre y la aplicación principal se desconecta.

En este caso, puede determinar rápidamente que los recursos informáticos ejecuten la aplicación u organicen la conmutación por error a los recursos de luz piloto en AWS. En este ejemplo, la base de datos secundaria almacena datos críticos. Si ocurre un desastre, el nuevo servidor web y el servidor de aplicaciones se inician y se conectan a la base de datos secundaria.
Amazon Route 53 está configurado para, posteriormente, dirigir el tráfico al nuevo servidor web.

El entorno principal puede existir en un centro de datos en las instalaciones o en otra región o zona de disponibilidad de AWS. Cualquiera sea el caso, puede utilizar el patrón de luz piloto para cumplir su objetivo de tiempo de recuperación (RTO).

PATRÓN DE LUZ PILOTO: LISTA DE COMPROBACIÓN

FASE DE PREPARACIÓN

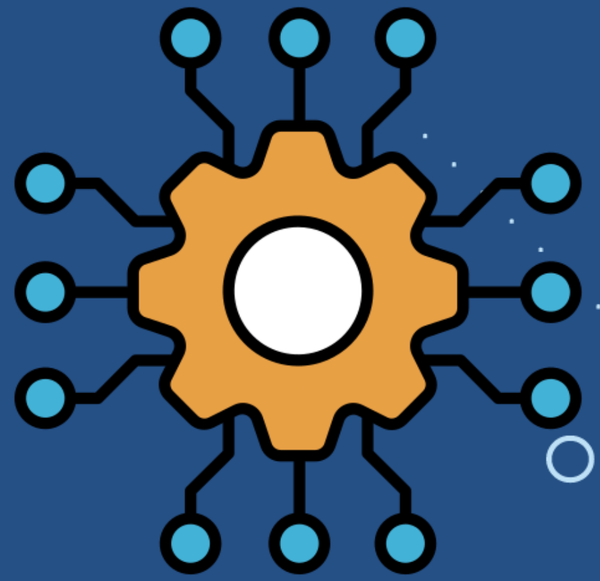
- Configure instancias EC2 para replicar o duplicar servidores.

- Asegúrese de que todos los paquetes de software personalizados compatibles estén disponibles en AWS.

- Cree y mantenga AMI de servidores clave donde se necesite una recuperación rápida.

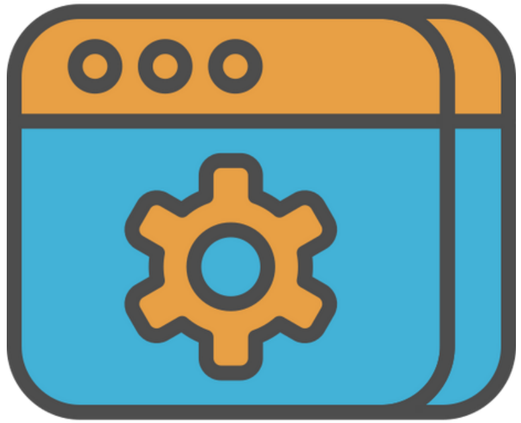
- Ejecute con regularidad estos servidores, póngalos a prueba y aplique todas las actualizaciones de software y los cambios en la configuración.

- Considere la posibilidad de automatizar el aprovisionamiento de recursos de AWS.



EN CASO DE DESASTRE

- **Active automáticamente los recursos en torno al conjunto de datos principal que se replicó.**
- **Amplíe el sistema según sea necesario para gestionar el tráfico de producción actual.**
- **Implemente el nuevo sistema.**
- **Ajuste los registros de DNS para que dirijan a AWS.**



COLOMBIA POTENCIA DE LA VIDA

TIC

Si implementa el patrón de recuperación de desastres de luz piloto, los pasos clave que debe completar durante la fase de preparación son los siguientes:

- Configure las instancias EC2.
- Asegúrese de que todos los paquetes de software personalizados compatibles estén disponibles.
- Cree y mantenga AMI esenciales donde se requiera una recuperación rápida.
- Ejecute y pruebe los servidores con regularidad, y aplique actualizaciones de software y configuración.
- Considere la posibilidad de automatizar el aprovisionamiento de recursos de AWS.

Si implementa el patrón de luz piloto, los pasos clave que debe completar si ocurre un desastre son los siguientes:

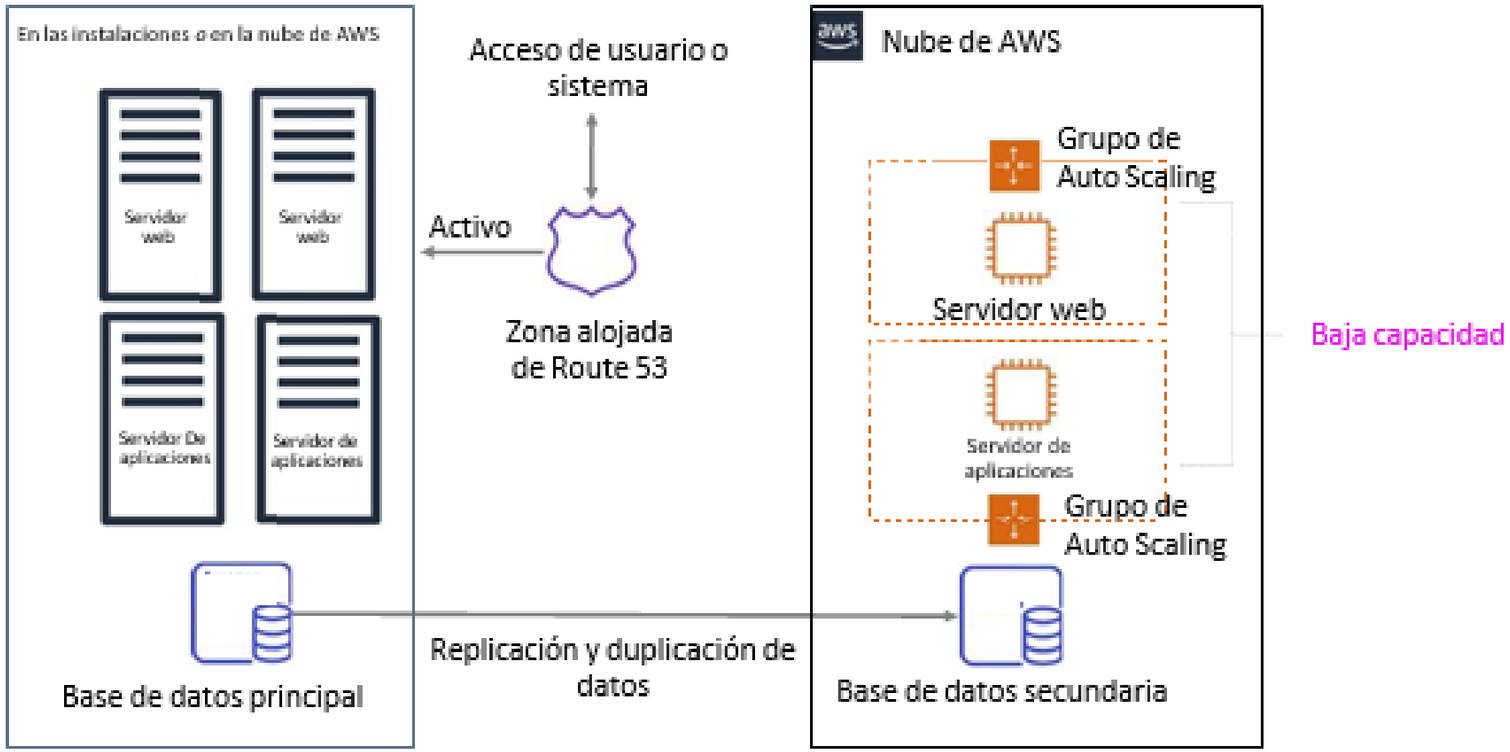
- Active automáticamente los recursos en torno al conjunto de datos principal que se replicó.
- Amplíe el sistema según sea necesario para gestionar el tráfico de producción actual.
- Implemente el nuevo sistema ajustando los registros de DNS para que dirijan a la implementación de copia de seguridad.

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

UTP Universidad Tecnológica de Pereira

PATRÓN DE ESPERA SEMIACTIVA: FASE DE PREPARACIÓN



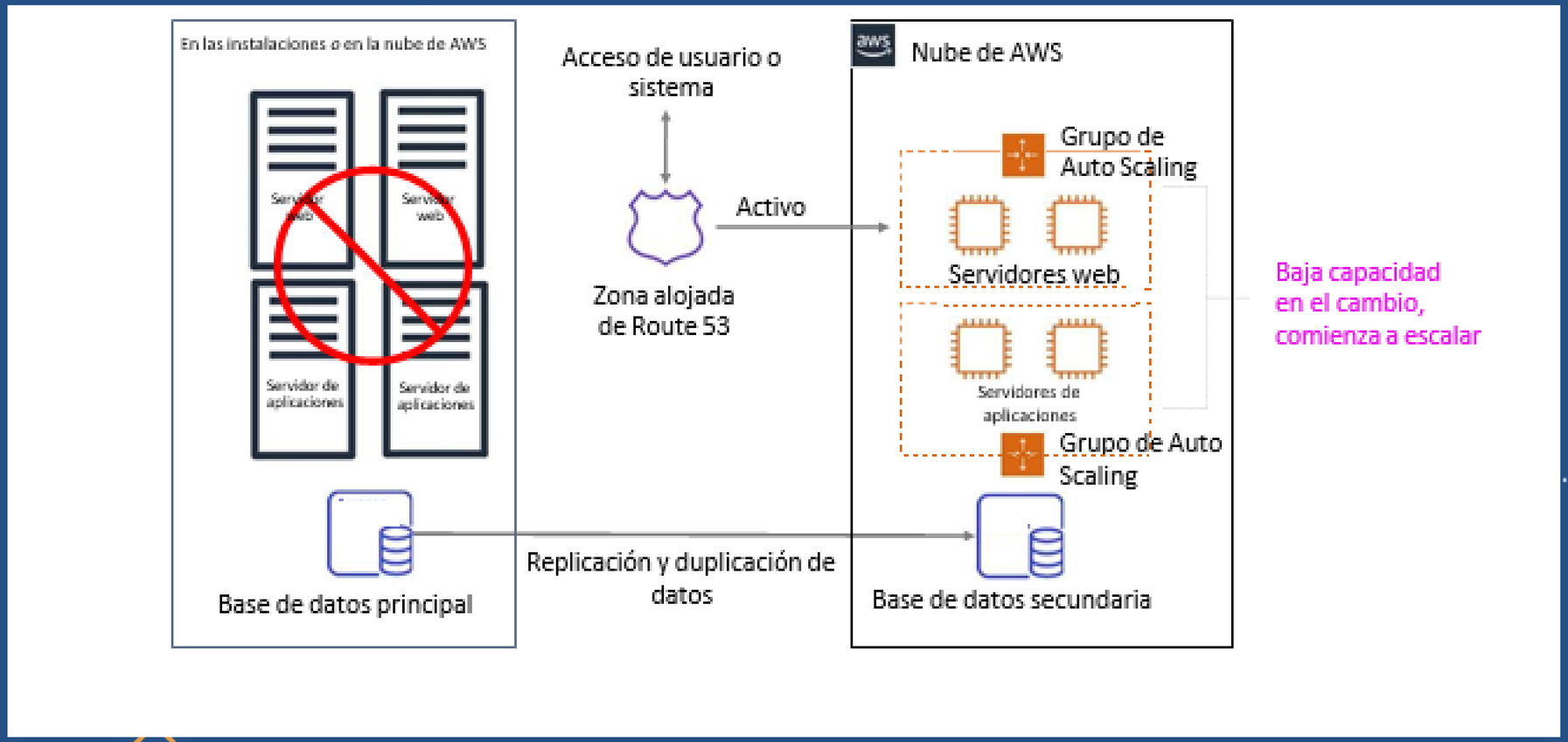
El tercer enfoque de recuperación de desastres es el patrón de espera semiactiva.

El patrón de espera semiactiva es como el de luz piloto, pero con más recursos ya en ejecución. El término espera semiactiva describe un caso de recuperación de desastres en la que siempre se está ejecutando una versión reducida de un entorno completamente funcional en la nube. La solución de espera semiactiva amplía los elementos y la preparación de luz piloto. Reduce todavía más el tiempo de recuperación porque algunos servicios siempre están en ejecución. Al identificar los sistemas que son críticos para la empresa, puede duplicarlos por completo y mantenerlos siempre activos.

Estos servidores pueden ejecutarse en una flota de instancias EC2 de tamaño mínimo, con los tamaños más pequeños posibles. Esta solución todavía no se ha ampliado para encargarse de una carga de producción completa, pero es totalmente funcional. Aunque originalmente se creó para fines de recuperación de desastres, también se puede utilizar para trabajos que no sean de producción, como pruebas, control de calidad y uso interno.

En el ejemplo, se están ejecutando dos sistemas. Es posible que el sistema principal se esté ejecutando en un centro de datos en las instalaciones o en una región de AWS, y un sistema de baja capacidad se está ejecutando en AWS. Utilice Amazon Route 53 para distribuir solicitudes entre el sistema principal y el de copia de seguridad.

PATRÓN DE ESPERA SEMIACTIVA: EN CASO DE DESASTRE



En un desastre, si el entorno principal no está disponible, Amazon Route 53 implementa el sistema secundario.

Así, el sistema secundario puede comenzar rápidamente a crecer por escalado vertical para gestionar la carga de producción. Puede producir este aumento agregando más instancias EC2 al balanceador de carga. O bien, puede modificar el tamaño de los servidores de poca capacidad para que se ejecuten en tipos de instancias EC2 más grandes. Se prefiere el escalado horizontal (crear más instancias EC2) al vertical (aumentar el tamaño de las instancias existentes).

COLOMBIA POTENCIA DE LA VIDA

TIC

PATRÓN DE ESPERA SEMIACTIVA: LISTA DE COMPROBACIÓN

PREPARACIÓN

- Similar al patrón de luz piloto

- Todos los componentes necesarios funcionan sin parar, pero no escalan en función del tráfico de producción.

- Práctica recomendada: pruebas continuas

- Filtre un subconjunto estadístico de tráfico de producción al sitio de recuperación de desastres.

EN CASO DE DESASTRE

- Conmute por error la carga de producción más esencial de inmediato

Ajuste los registros de DNS para que dirijan a AWS.

- Escale más (automáticamente) el sistema para que gestione toda la carga de producción.

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

UTP Universidad Tecnológica de Pereira

Si implementa el patrón de recuperación de desastres de espera semiactiva, la fase de preparación es importante. Los pasos clave que debería completar durante la fase de preparación son similares a los pasos que completa con el patrón de luz piloto. La diferencia más notable es que todos los componentes necesarios deben dejarse en ejecución ininterrumpida, pero no deben escalarse para el tráfico de producción.

Como práctica recomendada, realice pruebas continuas. También puede filtrar un subconjunto estadístico del tráfico de producción al sitio de recuperación de desastres. Así, puede verificar que funciona para usuarios y sistemas sin problemas al igual que el sistema primario.

1.

COLOMBIA POTENCIA DE LA VIDA

TIC

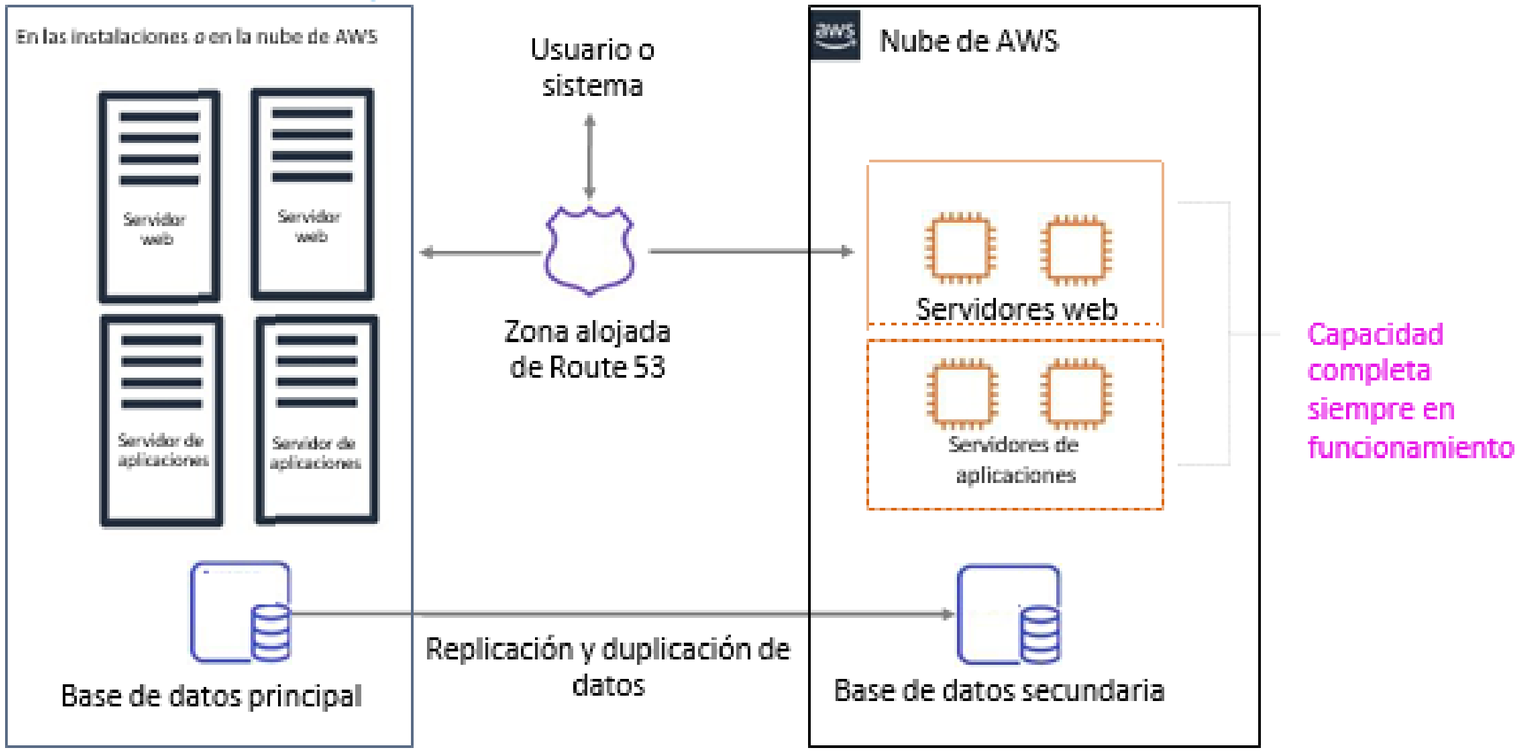
CON EL PATRÓN DE ESPERA SEMIACTIVA, SI OCURRE UN DESASTRE, LOS PASOS CLAVE QUE DEBE COMPLETAR SON LOS SIGUIENTES:

Realice la conmutación por error de la carga de producción más crítica, inmediatamente.

Ajuste los registros de DNS para que dirijan a AWS.

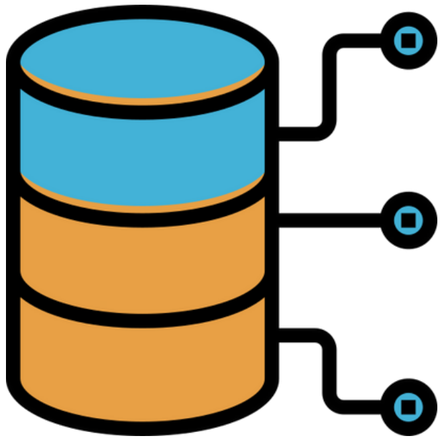
Escale más (automáticamente) el sistema para que gestione toda la carga de producción.

PATRÓN DE SITIOS MÚLTIPLES



El cuarto y último enfoque de recuperación de desastres es el patrón de sitios múltiples. Con este patrón, tiene un sistema completamente funcional que se ejecuta en una segunda región de AWS. Se ejecuta al mismo tiempo que los sistemas en las instalaciones o que los sistemas que se ejecutan en una región de AWS diferente.

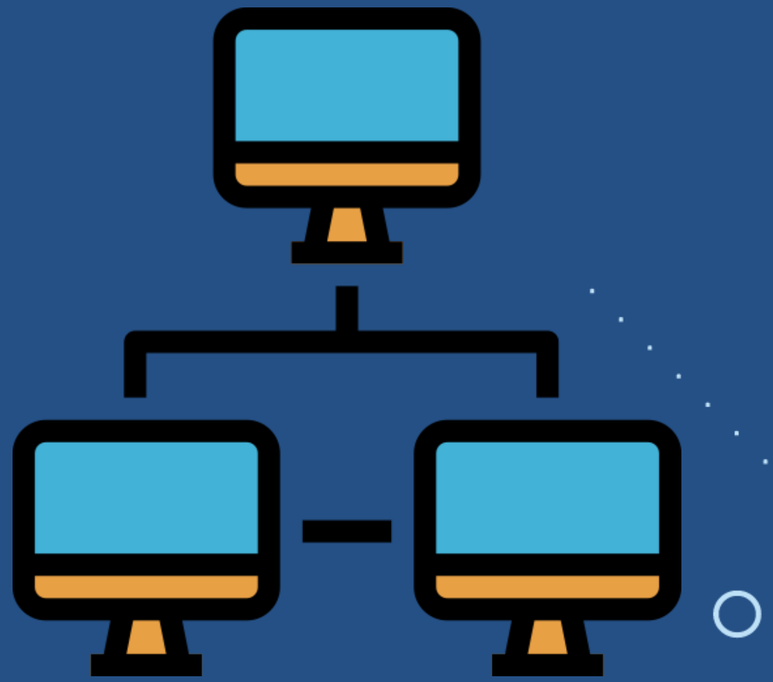
Una solución de sitios múltiples se ejecuta en una configuración activo-activo. El método de replicación de los datos que utiliza se determinada con el punto de recuperación que elija.



Dado que ambos sitios pueden admitir toda la capacidad de producción, puede optar por utilizar un servicio de DNS que admita el direccionamiento ponderado. Un ejemplo es Amazon Route 53, que dirige el tráfico de producción a ambos sitios que ofrecen la misma aplicación o servicio. En este caso, una parte del tráfico se lleva a la infraestructura de AWS y el resto, a la infraestructura en las instalaciones. (O bien, si los dos entornos están en regiones de AWS diferentes, el tráfico se distribuye proporcionalmente entre estas dos regiones).

En una situación de desastre en las instalaciones o en una región principal de AWS, puede ajustar la ponderación de DNS y enviar todo el tráfico a la segunda implementación. Así, la capacidad de la implementación secundaria se puede aumentar rápidamente para gestionar toda la carga de producción según sea necesario. Puede utilizar Auto Scaling de Amazon EC2 para automatizar este proceso. Es posible que necesite lógica de aplicación para detectar el error de los servicios de bases de datos principales y pasar a los servicios de bases de datos paralelos que ya se están ejecutando.

El costo de este caso se determina a partir del volumen de tráfico de producción que se observa durante el funcionamiento normal. En la fase de recuperación, solo paga por lo que usa durante el tiempo que se requiere el entorno de recuperación de desastres a escala completa. Puede reducir aún más los costos adquiriendo instancias reservadas de Amazon EC2 para los servidores de AWS que estén siempre activos.



SITIOS MÚLTIPLES: LISTA DE COMPROBACIÓN

PREPARACIÓN

- Similar a la espera semiactiva
- Configurado para el escalado horizontal total de la carga de producción

EN CASO DE DESASTRE

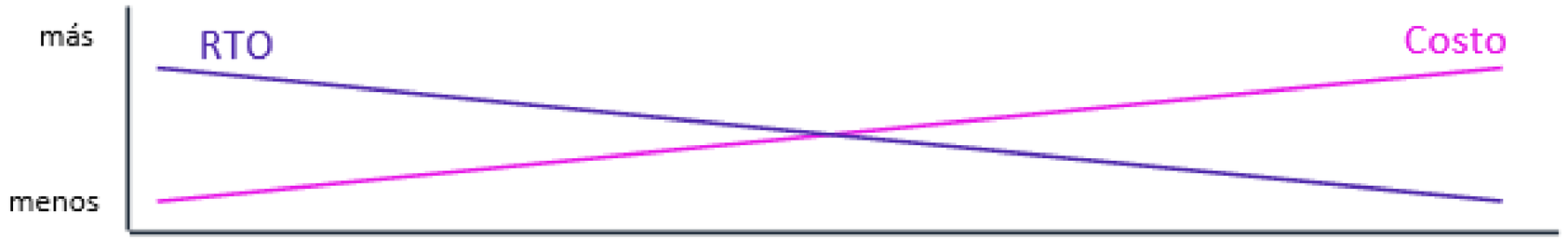
- Conmute por error de inmediato toda la carga de producción.

Si está implementando el patrón de recuperación de desastres de sitios múltiples, los pasos clave que debe completar durante la fase de preparación son similares a los del patrón de espera semiactiva. Debe configurar la implementación de la copia de seguridad de modo que se logre un escalado horizontal total de la carga de producción. Debe tener los servidores listos para recibir tráfico.

Con el patrón de sitios múltiples, si ocurre un desastre, solo necesita completar un paso clave. Este paso consiste en conmutar por error de inmediato toda la carga de producción al sitio de copia de seguridad.

Es posible que el patrón de sitios múltiples tenga el menor tiempo de inactividad de todos. Sin embargo, tiene más costos asociados porque presenta más sistemas en ejecución.

RESUMEN SOBRE LOS PATRONES COMUNES DE RECUPERACIÓN DE DESASTRES



Copia de seguridad y restauración	Luz piloto	Espera semiactiva	Sitios múltiples
▪ Casos de uso de menor prioridad ▪ Soluciones: Amazon S3, Storage Gateway	▪ Cumplimiento de requisitos de RTO y RPO más bajos ▪ Servicios principales ▪ Escalado de recursos de AWS en respuesta a un evento de recuperación de desastres	▪ Soluciones que requieren RTO y RPO en el marco de minutos ▪ Servicios críticos para la empresa	▪ Conmutación automática por error de su entorno en AWS a un duplicado en ejecución

En resumen, cada uno de los cuatro patrones de recuperación de desastres ofrece una combinación diferente de beneficios.

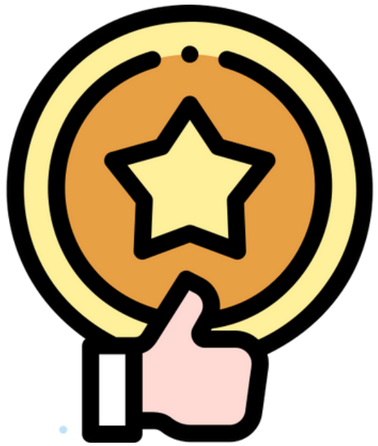
El diagrama muestra una gama para los cuatro casos, organizada de acuerdo con la rapidez con la que un sistema puede estar disponible para los usuarios después de un evento de recuperación de desastres.

El patrón de copia de seguridad y restauración normalmente se puede lograr al menor costo, pero tiene un RTO más prolongado. Como resultado, es probable que los sistemas se restauren más lento que con las otras opciones.

Los patrones de espera semiactiva y sitios múltiples admiten un RTO mucho más rápido, pero resulta costoso tener servidores adicionales que siempre se estén ejecutando.

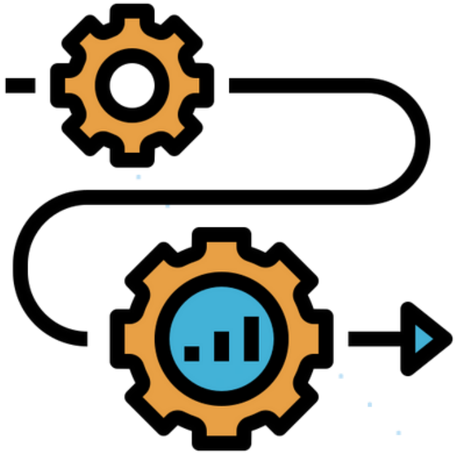
AWS le permite operar de forma rentable cada una de estas estrategias de recuperación de desastres. Es importante saber que estos patrones son solo ejemplos de posibles enfoques y que es posible combinarlos y generar variaciones. Si la aplicación se ejecuta en AWS, puede utilizar varias regiones y se seguirán aplicando las mismas estrategias para la recuperación de desastres.

PREPARACIÓN PARA LA RECUPERACIÓN DE DESASTRES: PRÁCTICAS RECOMENDADAS



COMIENCE DE MANERA SENCILLA

COMPRUEBE QUE NO HAYA NINGÚN PROBLEMA CON LAS LICENCIAS DE SOFTWARE



PRACTIQUE CON LOS EJERCICIOS DEL DÍA DE PRUEBAS

La creación de un plan integral para la recuperación de desastres puede ser una tarea compleja. Sin embargo, la mayoría de las organizaciones reconocen, tal vez por eventos pasados, que vale la pena el esfuerzo.

A pesar de que lleva tiempo desarrollar e implementar un plan completo, esto no debería impedirle dar algunos primeros pasos sencillos. Comience de forma sencilla y avance según sus necesidades. Por ejemplo, como primer paso, cree copias de seguridad de almacenamiento de datos, bases de datos y servidores críticos. Luego, trabaje para mejorar gradualmente el RTO y el RPO como un esfuerzo continuo.

Las licencias de software son un problema que puede surgir en la creación de sitios de copia de seguridad. Analice las licencias de software que tiene para determinar si sus contratos de licencia actuales admiten los planes de recuperación de desastres que ha desarrollado.
Actualice sus licencias o realice ajustes de alguna otra forma según sea necesario.

COLOMBIA POTENCIA DE LA VIDA

TIC

POR ÚLTIMO, UNA PRÁCTICA RECOMENDADA IMPLICA PONER A PRUEBA DE FORMA CONSISTENTE LA SOLUCIÓN DE RECUPERACIÓN DE DESASTRES PARA GARANTIZAR QUE FUNCIONE SEGÚN LO PREVISTO. ALGUNOS PASOS SUGERIDOS INCLUYEN LAS SIGUIENTES ACCIONES:

Practique con ejercicios de día de prueba. Estos ejercicios prueban casos en los que se desconectan sistemas críticos o incluso regiones enteras. ¿Qué pasa si deja de funcionar una flota entera?

Asegúrese de que se estén creando copias de seguridad, instantáneas y AMI, además de que estos recursos se puedan utilizar para restaurar los datos correctamente.

Controle su sistema de monitoreo.

Pruebe los procedimientos de respuesta para asegurarse de que sean efectivos y de que los equipos sepan cómo aplicarlos. Establezca días de prueba periódicos para medir la respuesta de las cargas de trabajo y el equipo ante eventos simulados.

ESTOS SON ALGUNOS DE LOS APRENDIZAJES CLAVE DE ESTA LECCIÓN:

- Los patrones de recuperación de desastres comunes en AWS incluyen copia de seguridad y restauración, luz piloto, espera semiactiva y sitios múltiples.
- Copia de seguridad y restauración es el enfoque más rentable, pero tiene el RTO más alto.
- Sitios múltiples ofrece el RTO más rápido, pero es el patrón más costoso porque proporciona un duplicado listo para la producción que se ejecuta en su totalidad.
- AWS Storage Gateway ofrece tres interfaces (gateway de archivos, gateway de volúmenes y gateway de cintas) para recuperar datos y realizar copias de seguridad entre las instalaciones y la nube de AWS.