Patrones y estrategías de DRP y Backups en la nube

Brayan Buitrago*

Guillermo Castro

César González

Escuela Colombiana de Ingenieria Julio Garavito

April 28, 2021

Abstract

La finalidad de este artículo es proponer una solución antes las diferentes problematicas o riesgos en la continuidad del negocio. Este articulo esta enfocado para cualquier tipo empresas. Todo Esto con la ayuda de las diferentes herramientas que se ofrecen los servicios en la nube, como lo son los Backup como servicio (BaaS) y los planes de recuperacion ante desastres como servicio (DRaaS) ***Palabras clave***

Backups, DRP, Nube Hibrida, Backups as a Service, Disaster Recovery as a Service .

I. Introducción

En la actualidad todas las empresas generan grandes cantidades de datos digitales e información, la cual es considerada como uno de los activos más importantes en cualquier tipo de organización. A medida que estas crecen requieren en mayor medida de los servicios de almacenamiento seguro y asegurar la disponibilidad inmediata de la información. Para aprovechar esta necesidad los proveedores de servicios administrativos presentan a las organizaciones de TI muchas opciones con respecto a la protección de datos, ya sea una infraestructura local tradicional o los servicios basados en la nube.

El tema de la continuidad del negocio es vital para el mantenimiento y sostenibilidad de estas empresas, cualquier tipo de fallo que afecte esto seria equivalente a grandes pérdidas economicas e incluso podría producir una posible quiebra. Por esto, se buscan soluciones que tengan una relación costo/beneficio para proteger el negocio y así verificar, sí realmente estamos preparados ante cualquier interrupción del servicio causado por diferentes factores como lo son: los errores humanos, algún desastre natural, outsiders insatisfechos y/o un ciberataque.

Se prioriza la protección de la infraestructura de TI y los datos en las empresas, lo cual les brinda la posibilidad de enfocarse netamente en lo que respecta a su modelo de negocio.Entre las soluciones que proponemos se encuentran los Backup como servicio (BaaS) y la recuperación ante desastres como servicios (DRaaS) que combinados conforman la estrategia de continuidad empresarial y recuperación ante desastres (BCDR), todo esto soportado en los servicios de la nube para satisfacer esta necesidad.

La organización requiere un Plan de Continuidad del Negocio (BCP) o un Plan de Recuperación ante Desastres (DRP) y una copia de seguridad de los datos que se encuentre dentro de las restricciones de costos

*A thank you or further information

mientras se cumplen los requisitos de recuperación en términos de objetivo de tiempo de recuperación (RTO) y objetivo de punto de recuperación (RPO). Se construira una guía que conduzca al uso y aprovechamiento de las tecnologías que provee la nube como backup y recuperación ante desastres tecnológicos en empresas colombianas.

II. Objetivos

Se plantean los siguientes objetivos a realizar:

- Entender las necesidades de las empresas en Colombia y visualizar su punto de vista ante los servicios que provee la nube.
- Comprender el funcionamiento de los mecanismos y las soluciones nativas de la nube, desde un punto de vista teórico, enfocado en las estrategias de recuperacion ante desastres.
- Elaborar una guía para la implementación del uso de los servicios en la nube como mecanismo de recuperación ante desastres tecnológicos enfocada en las empresas
- Implementar de manera practica e ilustrativa la guia anteriormente planteada

Text requiring further explanation[1].

III. Descripción del problema

Hoy en día existe el riesgo latente de que exista una caída o se tenga que enfrentar un desastre de cualquier indole, ya sea: desastre natural, ataque de algún usuario malintencionado o accidente de trabajo que produzca una interrupción en la continuidad del negocio es algo increíblemente costoso, más si no se tienen planes de acción ante estas situaciones. Muchas empresas cuentan todavía con infraestructura On Premise. Así que, las soluciones tradicionales de copias de seguridad locales fallan con mayor frecuencia a la hora de cumplir con los desafios y requisitos necesarios para mantener un negocio en la actualidad. La solución física sólo proporciona una funcionalidad límitada y en algunos casos puede presentar serias fallas de seguridad. Además, según varios estudios la mitad de las fallas son por causas "naturales" y la otra mitad se deben a fallas de componentes hardware o de software, incluyendo errores humanos. Algo importante es la seguridad del negocio y plantearse la pregunta ¿Cuáles son los dos ataques principales hacia la ciberseguridad o estado del negocio?

- Ransomware.
- Incidentes no planeados (fallas técnicas, desastres naturales).
- Errores humanos.
- Fallas imprevistas en el hardware.

Ransomware as a Service es la última tendencia en el mundo del ciberataque. Se han visto ejemplos muy representativos, como los ataques Wanna Cry y PetYa. Los ataques de Ransomware a dispositivos móviles y máquinas han aumentado un 250 durante los primeros tres meses de 2017, de acuerdo a un estudio realizado por Kaspersky.

Por lo general las empresas no cuentan con un personal de TI especializado, no están segmentadas por áreas, ya que, incluso una persona está a cargo de muchas funciones. Lo que implica de que sean las personas que corren mayor riesgo en caso de que ocurra un desastre. Por lo que sí está llegase a fallar ya sea en sólo cuestión de horas, o lo que tardé el recuperarse de la caída son pérdidas significativas en términos financieros. Los desastres naturales están a la orden del día en todo el mundo y los errores humanos y fallas de hardware nunca dejarán de existir.

IV. Marco Teórico

i. DRP

El DRP (Disaster Recovery Plan) o plan de recuperación de desastres te permite mantener esos sistemas informáticos críticos en dicha eventualidad. DRaaS es un servicio que complementa a BaaS, porque si bien la información se encuentra respaldada y podemos re-

[1] Example footnote

alizar restauraciones a nuestro sitio principal, no podemos recuperarnos de una falla completa. ¿A dónde restauraríamos la información si el backup server ya no existe?. Con DRaaS podemos tener una copia completa de las VM (Virtual Machines) productiva en el sitio de contingencia y encenderlas cuando sea necesario. Los mecanismos de software de algunos fabricantes permiten incluso encender las VM para pruebas sin afectar al productivo.

[scale=0.35]BAAS.png

ii. BaaS. Backup as a Service

Se trata de una tecnología que te permite resguardar tus respaldos en la Nube pública o Privada. ¿Cómo se hace? Requieres de 3 elementos:

Un software de respaldo y/o replicación en donde se alojará tu información.

Un Centro de Datos o Data Center que recibirá tu información en forma de respaldos, realizados precisamente por el software de respaldos o backup software.

Infraestructura dentro del Centro de Datos que guardará la información, almacenamiento y un poco de procesamiento para administrarlo.

Obviamente el Data Center será administrado por un proveedor de servicios o incluso puede ser un sitio alterno de tu propia organización. Solo ten presente que este último puede encarecer significativamente la solución.

[scale=0.35]BAAS.png

V. Estado del arte

i. Descripcion general

En la actualidad, el tema de las "caídas" y la recuperación de la información y continuación del negocio es algo primordial y de gran relevancia en temas de seguridad, pero a su vez es un aspecto tedioso y hasta cierto punto aburridor. Esta necesidad de conservar datos para su posible recuperación, ha adquirido protagonismo a causa de la gran cantidad de datos que llegan a recoger las empresas y usuarios en general.
La forma "tradicional" en que las empresas se apoyan para resguarar los datos y arhivos que crecen de manera exponencial, tienden a quedarse obsoletas y ponen en peligro desde las aspiraciones de crecer como organización hasta la misma continuidad de negocio. Ya que los famosos centros de datos (data centers), no estan diseñados para soportar las cantidades industriales de datos que se producen a diario. Los centros de datos modernos están atravesando una transformación tremenda, desde sistemas hiper-convergentes y código abierto hasta almacenamiento definido por el software (SDS, por sus siglas en inglés) y grandes sistemas escalables en la nube que las propias empresas pueden ensamblar. Esto sucede por la necesidad de agilidad comercial, alimentado por el software.
Las soluciones que aparecieron antes de los backups y DRP en la nube fueron tales como:

- La virtualización: A mediadios de los 60 fue una solución revolucionaria, ya que permitía recuperar sistemas duplicando imágenes de máquinas virtuales y replicándolas a otro lugar. Tenía la capacidad de reducir costes de infraestructura y era mucho más ágil que las soluciones físicas.
- El backup físico: Posteriormente salieron los sistemas de backup físicos, tanto en el sitio como remotos. Los remotos ofrecían más seguridad, aunque tenían costes prohibitivos para la mayoría de las empresas. Además, en el caso de un desastre, no eran capaces de garantizar una recuperación completa.

VI. Arquitectura

i. Azure Site Recovery

Site Recovery Service: la recuperación del sitio ayuda a mantener las aplicaciones comerciales y las cargas de trabajo en funcionamiento durante las interrupciones para garantizar la continuidad del negocio. Site Recovery replica

cargas de trabajo desde un sitio principal a una ubicación secundaria que se ejecuta en máquinas físicas y virtuales (VM). Cuando se produce una avería en el sitio principal, no puede ir a la ubicación secundaria y acceder a las aplicaciones desde allí. Es posible que no pueda volver a él después de que la ubicación principal se esté ejecutando nuevamente. Servicio de copia de seguridad: al realizar una copia de seguridad en Azure, el servicio AZURE Backup mantiene sus datos seguros y recuperables. Conjunto de disponibilidad: Azure garantiza que las máquinas virtuales que coloque en un conjunto de disponibilidad se ejecuten en varios servidores físicos, racks de cómputo, unidades de almacenamiento y conmutadores a la red. Si se produce una falla de hardware o software, solo un subconjunto de sus VM se verá afectado y su solución general permanecerá en funcionamiento. Los conjuntos de disponibilidad son fundamentales para el desarrollo de soluciones fiables en la nube.

[scale=0.5]prop1.png

ii. Copia de seguridad y recuperación ante desastres para aplicaciones de Azure

La recuperación ante desastres es el proceso de restaurar la funcionalidad de una aplicación a consecuencia de una pérdida catastrófica. en la nube somos conscientes de antemano de que se producirán errores. En lugar de intentar evitar todos los errores, el objetivo es minimizar los efectos que pueden provocar los errores de un único componente. La prueba es una manera de minimizar estos efectos. Debe automatizar las pruebas de las aplicaciones siempre que sea posible, pero debe estar preparado para cuando se produzca un error. Cuando esto sucede, es importante disponer de estrategias de copia de seguridad y recuperación.

El apetito al riesgo o la tolerancia al funcionamiento de la empresa, varia la necesidad que presenten las aplicaciones. En el caso de algunas aplicaciones, puede ser aceptable que no estén disponibles o que lo estén de forma parcial con funcionalidad reducida o retrasos en el procesamiento durante un tiempo. Sin embargo, en el caso de otras, cualquier funcionalidad reducida es inaceptable.

[scale=0.5]prp34.jpg

VII. Propuesta de solución

La solución a la problemática anteriormente presentada basada en alguna ventajas que logramos percibir a partir de la investigación realizada, y las cuales podemos presenciar en la figura 1 que se muestra posteriormente, seria enfocada a la migración de DRP y planes de continuidad del negocio ya que este es el principal problema que percibimos, Al tener una afectación de activos principales o joyas de la corona y no asegurar la triada de la ciberseguridad(Integridad, Disponibilidad y Confidencialidad), se presenta perdida valiosa de la información, afectando la reputación de la empresa.

La implementación de un Backup en la nube beneficiaria en varios aspectos a la recuperación del negocio ya que sería más eficiente y rápido ya que el servicio de la nube bien administrado, presenta alta disponibilidad alta confidencialidad y alta integridad. Finalmente, el almacenamiento en la nube de los activos permite realizar acciones preventivas para evitar la problemática que anteriormente se planteó.

Una de las posibles soluciones que analizamos, esta basado en el Site Recovery Azure o sitio de recuperacion de azure, el cual consiste en replicar las cargas de trabajo desde un sitio principal a una ubicación secundaria que se ejecuta en máquinas físicas y virtuales (VM).Grantizando la continuidad del negocio durante las interrupciones en el funcionamiento, generadas por las cargas de trabajo; Manteniendo en ejecucion constante las aplicaciones creadas en Azure.

Adicionalmente, Se deberia tener un plan de recuperacion de desastres, en el cual tengamos documentado el proceso a seguir para poder recuperar tanto el negocio como la aplicacion

o los servidores, usados en el momento de la creacion en azure para poder recuperar los activos perdidos o tener un tiempo eficiente de reactivacion del negocio.

VIII. Conclusiones

- Se logró promover la adopción de soluciones tecnológicas que potencialicen las capacidades de las compañías para lograr sus objetivos-
- Se Analizó la opción de guardar la información más valiosa para así tenerla disponible en cualquier momento, desde cualquier lugar y desde un sin número de dispositivos, siempre que estos estén conectados a internet
- Se evidencia que gracias a los backups el servicio siempre estara disponible,sera confidencial y presentara un entorno de integridad asi la demanda sea muy alta.
- Además de que las organizaciones aseguren de configurar correctamente los sistemas de Aws y tener un sitio de recuperacion en azure(Site recovery Azure) , también deberían utilizar tecnología de detección que permita detectar la explotación de alguna vulnerabilidad, los intentos de robo de credenciales y las configuraciones erróneas, que pueden dar lugar a que los atacantes expongan sus diversos secretos almacenados. Además, dado que los atacantes pueden modificar los conductos y desplegar malware o añadir cuentas para la persistencia, los equipos de Aws deberían buscar nuevos controles de seguridad, como la tecnología de engaño, para defender a Jenkins y a otras soluciones de Azure.

References

[1] IBM (2019) *Backup y Disaster Recovery Plan (DRP)*, IBM Cloud, Estados Unidos.

[2] Nubity (2018), *Backups físicos vs en la nube, nubity, Mexico .*

[3] HAROLD CASTRO. (2019). *Cloud Computing, Seminario internacional de computacion visual , Uniandes,Bogotá D.C.*

[4] Hassen Ben Rebah Hatem Ben Sta (2016) *Disaster Recovery as a Service: A Disaster Recovery Plan in the Cloud for SMEs,Conference:Global Summit on Computer Information Technology*