Polo del Conocimiento

Pol. Con. (Edición núm. 82) Vol. 8, No 6
Junio 2023, pp. 180-200
ISSN: 2550 - 682X
DOI: 10.23857/pc.v8i2

Estudio de mecanismos de contingencia en la nube para los servicios tecnológicos de un centro de datos en formación

Study of contingency mechanisms in the cloud for the technological services of a data center in training

Estudo de mecanismos de contingência na nuvem para os serviços tecnológicos de um data center em treinamento

Francisco Xavier Alvarez-Solis [I]
francisco.alvarezs@ug.edu.ec
https://orcid.org/0000-0002-2491-1162

Nelly América Valencia-Martínez [II]
nelly.valenciam@ug.edu.ec
https://orcid.org/0000-0001-6905-3125

Janeth Pilar Díaz-Vera [III]
janeth.diazv@ug.edu.ec
https://orcid.org/0000-0001-8750-0216

Alejandro Javier Gallegos-Arboleda [IV]
alejandro.gallegosa@ug.edu.ec
https://orcid.org/0009-0001-4770-1627

Correspondencia: francisco.alvarezs@ug.edu.ec

Ciencias de la Computación
Artículo de Investigación

*** Recibido:** 23 de abril de 2023 ***Aceptado:** 12 de mayo de 2023 *** Publicado:** 01 de junio de 2023

I. Docente Universidad de Guayaquil, Ecuador.
II. Docente Universidad de Guayaquil, Ecuador.
III. Docente Universidad de Guayaquil, Ecuador.
IV. Estudiante Universidad de Guayaquil, Ecuador.

Resumen

La Recuperación en caso de la afectación de los Servicios, siempre ha sido una preocupación constante, entre los Administradores de la Tecnología de la Información, pero es recién en los últimos años, con los continuos avances de la Informática en la Nube, en que su implementación generalizada, se ha vuelto viable. En el caso del Centro de Datos de la Carrera de Software, que está en su etapa inicial, se requiere conocer las alternativas existentes en nuestro mercado, para una implementación posterior, lo cual nos conduce a estudiar las características técnicas, operativas y financieras de los servicios DRaaS (Disaster Recovery as a Services) de los tres proveedores de informática en la Nube, con mayor participación del mercado mundial. Esto nos permite elaborar un cuadro comparativo que resume la información obtenida, y que es una guía para un análisis posterior, relacionado con las necesidades de la organización y del Centro de Datos. Este trabajo incluye una prueba de concepto, de los servicios DRaaS de uno de estos tres proveedores, cuyos resultados fueron muy aleccionadores. La conclusión general del estudio realizado es que se confirma la viabilidad financiera, técnica y operativa, de la implementación de los mecanismos de contingencia contenidos en los servicios DRaaS, para las empresas de todos los tamaños. También, se deja establecida la necesidad de que, la selección del proveedor de este servicio para esta organización incluya la obligatoriedad de realizar una prueba de concepto de todas las alternativas ofrecidas. Omitirla, es un factor de riesgo importante. Finalmente, es necesario ejecutar proyectos subsecuentes, que continúen, complementen y amplíen los resultados obtenidos con el presente estudio.

Palabras Clave: Contingencia; DRaaS; Nube; Recuperación; Resiliencia; RPO; RTO.

Abstract

Recovery in case of affectation of Services has always been a constant concern among Information Technology Administrators, but it is only in recent years, with the continuous advances in Cloud Computing, that its widespread implementation, it has become feasible. In the case of the Data Center of the Software Career, which is in its initial stage, it is necessary to know the existing alternatives in our market, for a later implementation, which leads us to study the technical, operational and financial characteristics of the DRaaS (Disaster Recovery as a Services) services from the three cloud computing providers with the largest global market share. This allows us to prepare a comparative table that summarizes the information obtained, and that is a guide for

further analysis, related to the needs of the organization and the Data Center. This work includes a proof of concept, of the DRaaS services of one of these three providers, whose results were very instructive. The general conclusion of the study carried out is that the financial, technical and operational viability of the implementation of the contingency mechanisms contained in the DRaaS services is confirmed for companies of all sizes. Also, the need is established for the selection of the provider of this service for this organization to include the obligation to carry out a proof of concept of all the alternatives offered. Omitting it is an important risk factor. Finally, it is necessary to carry out subsequent projects, which continue, complement and expand the results obtained with the present study.

Keywords: Contingency; DRaaS; Cloud; Recovery; Resilience; RPO; RTO.

Resumo

A recuperação em caso de afetação de Serviços sempre foi uma preocupação constante entre os Administradores de Tecnologia da Informação, mas somente nos últimos anos, com os contínuos avanços da Computação em Nuvem, é que sua ampla implementação se tornou viável. No caso do Data Center da Carreira Software, que se encontra na sua fase inicial, é necessário conhecer as alternativas existentes no nosso mercado, para uma posterior implementação, o que nos leva a estudar as características técnicas, operacionais e financeiras do Serviços DRaaS (Disaster Recovery as a Services) dos três provedores de computação em nuvem com a maior participação no mercado global. Isto permite-nos preparar um quadro comparativo que sintetiza a informação obtida, e que serve de guia para análises posteriores, relacionadas com as necessidades da organização e do Data Center. Este trabalho inclui uma prova de conceito, dos serviços DRaaS de um destes três provedores, cujos resultados foram bastante instrutivos. A conclusão geral do estudo realizado é que se confirma a viabilidade financeira, técnica e operacional da implantação dos mecanismos de contingência contidos nos serviços DRaaS para empresas de todos os portes. Também se estabelece a necessidade de a seleção do prestador deste serviço para esta organização incluir a obrigação de realizar uma prova de conceito de todas as alternativas oferecidas. A omissão é um importante fator de risco. Por fim, é necessário realizar projetos posteriores, que dêem continuidade, complementem e ampliem os resultados obtidos com o presente estudo.

Palavras-chave: Contingência; DRaaS; Nuvem; Recuperação; Resiliência; RPO; RTO.

Introducción

El estudio de los mecanismos de contingencia en la nube pública, que se realizó con este trabajo, es posible asociarlo con la practica denominada, en ITIL V4 (AXELOS Limited, 2019, p.151), como "Gestión de Disponibilidad", Allí se define a la Disponibilidad como "La capacidad de un servicio de TI u otro elemento de configuración para realizar su función acordada cuando se requiera". Adicionalmente, es preciso destacar que, en la Norma ISO 27002:2022 (International Organization for Standardization, 2022, p.8) se establece que la Disponibilidad es una de las propiedades de la Seguridad de la Información (p.8), o sea que es uno de los tres atributos mediante el cual se puede establecer si los diversos controles ayudan a preservarlo o no.

Las consideraciones para la Disponibilidad están presentes en todo servicio que está funcionando, ya que, ante la presencia de eventos que perturben o afecten su estabilidad, es necesario actuar para que los servicios tecnológicos que se están entregando no se interrumpan. Acorde con Chakraborty & Chowdhury (2020). se pueden tener fallas de distinto origen:

Amenazas físicas (fallas de Hardware, interrupción del servicio de energía eléctrica, eventos naturales, terrorismo, huelgas, etc.) y amenazas lógicas (fallas del Software, ataques de programa maligno o ransomware, degradación del rendimiento, corrupción de los archivos, etc.).

Es en el momento en que se presenta alguna de las fallas mencionadas, que las actividades que son propias de la práctica de la Gestión de la Disponibilidad y de la Continuidad del Negocio (análisis de riesgos, su mitigación, planificación para saber qué hacer ante la ocurrencia de eventos contingentes, la ejecución de las medidas de prevención, etc.), cobran una gran importancia para sostener los planes operativos y estratégicos de las organizaciones.

Acorde con Terinte (2018) y de las revisiones efectuadas de los distintos ofrecimientos de los proveedores de la nube pública, se ha encontrado con que, el actual nivel de madurez tecnológica y de economía de escala, que han alcanzado en estos servicios, los hace una opción muy natural para la recuperación en caso de contingencias o desastres, sobre todo, si se la compara con la clásica acción de construir un Centro de Datos alterno para recuperar los servicios, que es una solución de que requiere inversiones considerables para su construcción y operación.

Por esa razón, este estudio, se ha realizado con la idea de sistematizar la información disponible y relacionada con los mecanismos de contingencia que ofrezcan los distintos proveedores de la nube y, de esta manera, confirmar los beneficios y bondades que ofrecen estos servicios de contingencia,

facilitar su utilización, para encontrar el proveedor idóneo que atienda las necesidades de recuperación, para el Centro de Datos de la Carrera de Software.

Conceptos fundamentales

Dado que este estudio es acerca de los mecanismos de contingencia que ofrecen los proveedores de servicio de la nube pública, encaja en una de las facetas de la Tecnología de Información y Comunicaciones (TIC), que es el que enfrenta el desafío de entregar los servicios, sin interrupciones a los usuarios o, al menos, de mantenerlos disponibles durante la máxima cantidad de tiempo que sea posible.

Trabajar en la optimización de la disponibilidad de los servicios, es un imperativo muy desarrollado en las organizaciones y empresas de la época presente. En las TIC's se la encuentra en la redundancia de los componentes que forman parte de los servicios, por ejemplo, servidores con doble fuente de poder, UPS's configuradas con una UPS adicional (se las llama N+1), rutas de enlaces de comunicaciones redundantes, servidores en clúster, etc. Esto se hace necesario, ya que, desde que las organizaciones fueron avanzando en el uso de las TIC's para optimizar sus operaciones y adquirir ventajas competitivas, el impacto de las interrupciones en los servicios, se hace cada vez mayor e implica inaceptables costos financieros y de imagen ante el mercado.

La evolución que han seguido todas las medidas y procesos destinados a maximizar la disponibilidad e, incluso, a planificar la recuperación de los servicios, ha dado lugar, a que estas consideraciones se apliquen a todo el entorno en el que actúan las organizaciones, no solamente a las TIC's

Así, desde hace relativamente poco tiempo, se ha desarrollado la denominada Resiliencia Empresarial, la misma que, a más de los avances que se han dado con la disponibilidad de las TIC's, contempla de manera integral, otras áreas. En este apartado, explicaremos los conceptos relacionados con ella. Posteriormente, detallaremos las nociones relacionadas con los Servicios en la Nube.

Gibbs et al, (2022), nos plantean considerar la siguiente definición de Resiliencia:

Nos referimos a la resiliencia como un proceso dinámico definido por la Estrategia Internacional para la Reducción de Desastres de las Naciones Unidas (UNISDR) como "la capacidad de un sistema, una comunidad o una sociedad expuesta a peligros para resistir, absorber, acomodarse y

Pol. Con. (Edición núm. 82) Vol. 8, No 6, Junio 2023, pp. 180-200, ISSN: 2550 - 682X

recuperarse de los efectos de un peligro de manera oportuna y eficaz, incluso mediante la preservación y el restablecimiento de sus estructuras y funciones básicas esenciales" (p. 2).

El siglo XXI, desde sus inicios, se ha caracterizado por ser una era de incertidumbre económica y geopolítica. En Wolbers, J., Kuipers, S., & Boin, A. (2021) se registran varios incidentes de gran impacto: el ataque a las torres gemelas del 11 de septiembre/2001, el tsunami en el Océano Indico (2004), el Huracán Katrina (2005), la crisis económica y financiera de 2008, la erupción volcánica en Islandia 2010), el terremoto de Japón, en 2011 que provocó daños en la Central Nuclear de Fukushima, los ataques terroristas en diversas partes del mundo, el cambio climático, la pandemia de COVID-19 (2020-2022) y más recientemente, la Guerra entre Rusia y Ucrania (Brende & Sternfels, 2022, p. 5) Todos ellos han perturbado o perturban aun, el funcionamiento de las organizaciones que operan en su área de impacto; en particular los dos últimos casos, han implicado una afectación global, en todas partes del planeta. En Aldea, A., Vaicekauskaitė, E., Daneva, M., & Piest, J. P. S. (2021) se establece que, en los días presentes, esto se ha manifestado mediante el impacto a la cadena de suministro de los productos de tecnología, tales como computadores, teléfonos y otros equipos de redes y comunicaciones. (Sanchis & Poler, 2020)

En Sanchis & Poler (2020), se plantea que si a esto, además se agrega las transformaciones que ha sufrido el mercado., esto es, mercados y clientes más exigentes, la velocidad con que se desarrollan o evolucionan las tecnologías, entonces se puede apreciar la necesidad, en el afán de sobrevivir y crecer, de desarrollar la resiliencia de manera integral, que cubran todas las áreas del entorno de las organizaciones, (p. 502).

Sanchis & Poler, (2020) nos dicen que

“El estudio de la resiliencia aplicado al mundo empresarial ha ido creciendo en las últimas décadas debido al gran dinamismo del entorno en el que operan las compañías. Áreas afines a la gestión de la resiliencia como la gestión de riesgos, la continuidad del negocio, la recuperación ante desastres, no han ido evolucionado a la misma velocidad con la que las empresas precisan para lidiar con las amenazas del entorno y con las situaciones de crisis. Es por ello por lo que nace la gestión de la resiliencia como un nuevo enfoque en el que se definan y desarrollen nuevas herramientas que complementen a los enfoques tradicionales para satisfacer las necesidades actuales y el carácter dinámico del entorno en el que las empresas operan (Sanchis & Poler, 2019a)” (p.502)

En la Figura 1, vemos algunas de las clases de resiliencia que se han desarrollado conceptualmente y su relación con la Resiliencia Empresarial (en inglés, Organizational Resilience)

Figura 1 - Relaciones entre conceptos de resiliencia y la resiliencia organizacional

Fuente: Adaptada de Ruiz-Martin et al , 2018, p. 12

Resiliencia y Sistemas de información

La mayoría de las organizaciones, dependen de los Sistemas de Información, para la realización de sus operaciones. En el caso de que hubiera una disrupción significativa, en los sistemas de información, habría un impacto muy alto en sus actividades, ya que muchas de las tareas se tendrían que realizar manualmente y/o en papel. Imaginemos al correo en cartas o la contabilidad registrada en libros de papel, por mencionar los casos menos complejos. Por esta razón, cuando se planifican las actividades durante las crisis en las organizaciones, es de la máxima importancia, examinar la continuidad de los servicios clave de los Sistemas de Información.

Gestión de la continuidad del negocio

Crask, 2021 establece que, el término “Continuidad del Negocio se usa para describir la capacidad de una organización, para continuar o recuperar las operaciones, que después de un incidente disruptivo” (p. 4). El mismo autor plantea que la Resiliencia Organizacional, es un concepto que se usa para describir un enfoque integrado para brindar la continuidad del negocio, junto con aspectos que muchas organizaciones considerarían parte de la Gestión del riesgo operacional

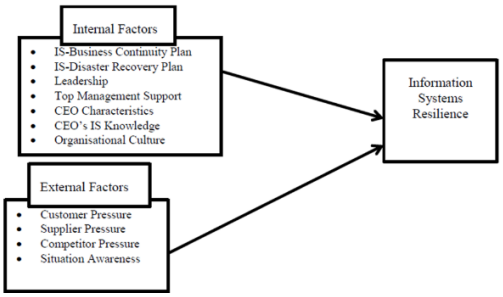

Figura 2 - Marco conceptual para los Sistemas de Información

Fuente: Sarkar, Wingreen, & Cragg, 2013

Se puede apreciar que, entre los factores internos, se incluyen los Planes de Continuidad del Negocio y los Planes de Recuperación ante Desastres.

La Gestión de la Continuidad del Negocio, está regulada por una familia de normas, que están bajo la responsabilidad del Comité Técnico 292 (Technical Committee, TC 292) de la ISO, que tiene a su cargo toda la normativa que se relaciona con la Seguridad y la Resiliencia:

La realización de un Plan de Continuidad del Negocio requiere que se haga lo siguiente:

● identificar los procesos y actividades que se considera prioritarios y críticos para que la organización mantenga sus operaciones y pueda entregar sus productos y servicios;

● identificar los recursos que son necesarios para entregar estos procesos y actividades críticos;

● elaborar y mantener todos los planes de continuidad del negocio, gestión de incidentes y gestión de crisis, de modo que la organización pueda responder a todos los impactos que se ocasionan luego de una interrupción o crisis;

● capacitar al personal que deberá ejecutar el Plan de continuidad del negocio;

● realizar pruebas periódicas del Plan de Continuidad del Negocio validar la efectividad de los planes de respuesta y recuperación de la organización;

● aplicar un proceso de mejora continua para asegurar que las capacidades de continuidad del negocio permanezcan actualizadas y sean útiles para la organización.

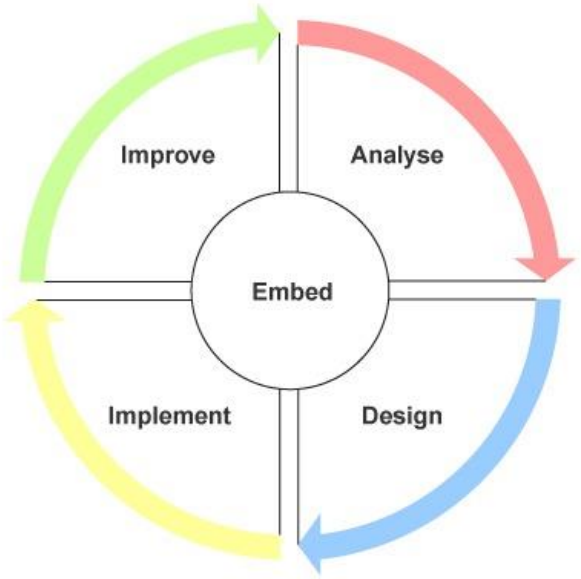

Figura 3 - Ciclo de Vida de la Gestión de la Continuidad del Negocio

Fuente: Adaptada de Crask, 2021, p. 7

1.-Analizar: Es el primer paso. Aquí se realiza el análisis del impacto en el negocio para identificar los procesos y actividades críticos de la organización y determinar las prioridades de recuperación. Los errores u misiones que se cometan en esta fase crucial podrían resultar en la elaboración de planes de recuperación incompletos.

2.-Diseñar: esta se definen las estrategias de recuperación y la forma en que se obtendrán los recursos que necesitan los procesos y actividades críticos. Por ejemplo, estos recursos pueden ser el personal formado necesario para desempeñar una función concreta, un sistema informático, datos, un proveedor externo o un edificio específico.

Las estrategias y soluciones de recuperación desarrolladas aquí constituyen la base de lo que se documentará en los planes de recuperación y deben garantizar que todos los procesos y actividades críticas puedan recuperarse en los plazos acordados y con las capacidades esperadas.

3.-Implementar: Los resultados de las dos primeras etapas del ciclo de vida proporcionan gran parte de los detalles que se necesitarán para desarrollar el plan, lo que se hará en esta etapa.

4.-Mejorar: Para mejorar el Plan realizado, se incluirán revisiones de la dirección, auditorías, informes posteriores a los incidentes y, se realizar las pruebas del Plan, diseñadas para validar la eficacia de este. Cada vez que se identifique una mejora a través de los procesos implementados

en esta etapa garantizan que las disposiciones de la organización se actualicen para para reflejar los últimos aprendizajes y las buenas prácticas.

5.-Incorporar: esta etapa se centra en la formación del personal para garantizar que son capaces de cumplir eficazmente con sus deberes de continuidad de la actividad de la continuidad de la actividad, pero también incluye la concienciación del personal de la plantilla, en general.

Variables de la investigación

Todo diseño e implementación de soluciones, relacionada con mecanismos de contingencia, tiene como elementos característicos, las necesidades específicas que se tengan en relación con los tiempos de recuperación y la cantidad de datos que se considera aceptable que no estén actualizados.

Con ese fin, en forma general, se han definido dos variables que, en su conjunto, van a cubrir las necesidades realistas que tenga cada organización particular. Dado que estas variables, son definidas para analizar diferentes escenarios que cubran las necesidades de recuperación de la organización, se las considera.

Variables Independientes

La primera variable, es el Objetivo de Tiempo de Recuperación (Recovery Time Objective, RTO) La norma ISO 22300 la define como “periodo de tiempo tras un incidente en el que se reanuda un producto o servicio o una actividad se reanuda, o se recuperan los recursos” (p.23)

Una vez que ocurre la interrupción de los servicios, por un mal funcionamiento o por un desastre, la organización debe trabajar para que los servicios vuelvan a estar disponibles, en el menor tiempo que sea posible. A este fin, con RTO se define el tiempo máximo de tolerancia en que la organización está dispuesta a esperar, hasta que el servicio se restablezca, sin que se cause un daño a su imagen o reputación comercial, operativa o financiera.

Hay casos en los que las interrupciones pueden ocurrir por varios días, sin que haya ningún tipo de consecuencias, y otros casos en los que una interrupción de pocos segundos puede causar reclamos o inconformidad de los clientes. Imaginemos, una interrupción de Netflix o de Google de pocos segundos o minutos. Con seguridad, ocasionaría malestar y/o reclamo de los clientes o usuarios.

La determinación de RTO, se debe realizar para todos y cada uno de los servicios que están activos en producción. Esto se lo realiza en la fase de inicial del Plan de Continuidad de Negocio, que se denomina Análisis de Impacto en el Negocio (en inglés, Business Impact Analysis, BIA).

La segunda variable, es el Objetivo de Punto de Recuperación (Recovery Point Objective, RPO)

La norma ISO 22300 la define como "punto en el que se restablece la información utilizada por una actividad para que ésta pueda funcionar en la reanudación" (p.23)

La actividad de respaldo de la información es una práctica muy madura y establecida en los Centros de Datos. Se la realiza con la finalidad de preservar los datos vigentes en un momento específico del tiempo, y brinda la posibilidad de que pueda ser utilizada en caso de que se produzca algún inconveniente que afecte la disponibilidad de los datos.

Por lo general, los respaldos se realizan con una frecuencia previamente establecida; por ejemplo, más de una vez en el día, con respaldos completos o parciales (diferenciales o incrementales).

Esto nos conduce a la situación de que, una vez que se produzca la interrupción del servicio, o el desastre, solamente contaremos con los datos que constan en el último respaldo obtenido. Los datos que se ingresaron, que se modificaron o eliminaron, después de ese último respaldo, por lo tanto, se perderán,

El Objetivo de Punto de Recuperación, por lo anterior, nos indica cual es la cantidad de datos que la organización está dispuesta a tolerar que se pierdan, ante la ocurrencia de una contingencia.

Los datos de los servicios más críticos se deben respaldar con mayor frecuencia que aquellos que son de importancia menor. Los servicios con RPO cercano a cero, requieren que los respaldos se realicen mediante el esquema de conmutación por error o de replicación constante. En sentido opuesto, los respaldos menos frecuentes, conllevan la definición de un RPO más grande.

La siguiente figura, nos ayuda a relacionar estas dos variables independientes, RTO y RPO, en relación con el momento en que se produce la interrupción no planificada (o desastre) del servicio.

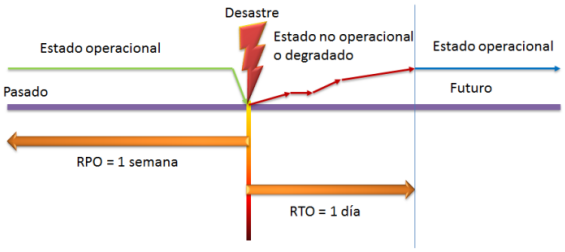

Figura 4 - Relación de RPO y RTO con el inicio del desastre.

Fuente: Revista Datacenter, 2013

Aquí, se puede apreciar que, los respaldos solamente se realizan 1 vez por semana (RPO) y que el RTO es de 1 día, esto es, los servicios serán restaurados hasta 1 día después de que ocurrió el desastre.

Variables Dependientes

Una vez que se han definido el RTO y el RPO, para atender las necesidades de recuperación de la Organización, se deben implementar las soluciones que permitirán cumplir con los valores definidos.

Figura 5 - El Costo de Implementación del Mecanismo de Contingencia – Variable dependiente

Fuente: Arnal Zaragozá (2020)

En consideración de que, generalmente se necesita recuperar la infraestructura, el costo de la recuperación crecerá exponencialmente, cuando se trata de atender un requerimiento de RTO cercano a cero. Las inversiones y gastos por efectuar son considerables. Cuando se cuenta con un RTO mayor, la inversión y gastos a considerar, son menores.

Este razonamiento, es similar para el caso de tener que diseñar una solución que permita cumplir con el RPO definido

Por lo expuesto, resulta evidente que es válido considerar al COSTO de implementación de las medidas de recuperación ante las contingencias (o Desastres) como la variable dependiente de este estudio. El Costo, depende de las definiciones que se hayan hecho de RTO y RPO.

Como se puede apreciar en la Figura 5, el punto de equilibrio que se genera en la intersección de las 2 curvas nos entrega el monto de inversión óptima y el valor de RPO y RTO que se podría generar con esa inversión. Desde luego, la definición de RPO y RTO inicial, debe ser del objetivo prioritario, porque se definen considerando la magnitud del impacto financiero y la afectación a la imagen y reputación de la empresa.

Resultados

Este estudio nos ha permitido conocer los detalles más importantes que conforman los servicios de Recuperación ante Desastres (DRaaS), que ofrecen los tres principales proveedores de la nube con cobertura mundial y que operan en el Ecuador

En forma general, la investigación realizada, brinda una sólida evidencia de que ahora, con la disponibilidad de los servicios de contingencia en la nube que se han revisado, prácticamente todas las empresas, de cualquier nivel (microempresa, pequeña, mediana y grande), están en condiciones de mejorar la resiliencia de sus negocios, implementando los planes de recuperación de los servicios y la infraestructura tecnológica que le permita mantener activa su operación, a pesar de que se presenten incidentes que tengan un impacto considerable en la disponibilidad de sus servicios de Tecnología de la Información y Comunicaciones.

Este resultado se sustenta en que, es posible comenzar con una cantidad mínima de servicios tecnológicos o equipos servidores (podrían ser tan solo un servicio, con un único equipo servidor), elegidos de acuerdo a las necesidades o conveniencias de la empresa que los usa- Esto, permite ganar conocimiento y experiencia en las actividades de planificación para recuperarse ante desastres, en la prueba de esos planes y, en el caso de que se ocurra alguna interrupción, en la ejecución de esos planes. Todo esto, con una pérdida de datos (RPO) muy pequeña (que puede reducirse a segundos), con tiempos de recuperación (RTO) del orden de minutos y sin necesidad de tener que superar curvas de aprendizaje largas, complejas y costosas.

Posteriormente, se puede ir ampliando, de una forma muy sencilla, la cobertura de los servicios tecnológicos a proteger con estos mecanismos de contingencia, hasta llegar a cubrir la totalidad de

las necesidades prioritarias de recuperación que tenga la empresa. Asimismo, en cada ocasión en que se incrementen o se incluyan más servicios tecnológicos en el proceso de recuperación, también se deben probar, con una frecuencia semestral, el correcto funcionamiento de la recuperación que se ha planificado, para la totalidad de los servicios incluidos. Ahora, a diferencia de lo que ocurría hace poco tiempo atrás, estas pruebas se pueden realizar, sin que se tenga que interrumpir ninguna de las operaciones de la empresa.

Otro factor que impulsa la adopción de los servicios de contingencia o recuperación en la nube, es que antes de la disponibilidad de estos servicios en la nube, se tenía que seleccionar, diseñar o construir, un centro de datos alterno, para que pueda ser usado, en el momento en que se presente una afectación a la disponibilidad de los servicios, Obviamente, en muchas ocasiones, esto requería que las empresas, realicen inversiones de montos considerables, tanto para la construcción, como para el equipamiento del centro alterno. De aquí, se derivaban otras necesidades, tales como instalar y configurar los equipos del Centro de Datos alterno; luego, cuando se producían cambios en la infraestructura del Centro de Datos principal, también se debían actualizar los componentes instalados en el Centro de Datos alterno. Otro detalle que había que tener consideración, es la frecuencia con que se actualicen los datos en los equipos alternos. Por lo general, en la gran mayoría de los casos, las pruebas de los planes de recuperación obligaban a interrumpir las operaciones de la empresa

En el caso de que se empleen los mecanismos de contingencia disponibles en las empresas en el mercado ecuatoriano, los precios a pagar por cada equipo que deba recuperarse o por la infraestructura o los servicios en la nube, que deban utilizarse, están en el orden de magnitud de unos pocos cientos de dólares por mes, por cada equipo, los cuales en el modelo de precios que aplican los proveedores en la nube, solamente se deberán pagar, cuando sean usados. Esto es un contraste significativo con la situación vigente en la época anterior a la disponibilidad de la informática en la nube, en que se tenían que invertir varias decenas o centenares de miles de dólares que debían agregarse a los gastos recurrentes que estaban relacionados con el pago por el mantenimiento de los equipos, energía eléctrica, aire acondicionado, videovigilancia, etc. del Centro de Datos alterno.

Por otro lado, los tres proveedores investigados (AWS, y AZURE y GOOGLE) cuentan con una arquitectura estable y de utilización sencilla. Cada uno tiene su enfoque particular, para replicar los

datos en su infraestructura de la nube y para la ejecución de los procesos de conmutación por error (Failover) y de conmutación por recuperación (Failback).

Con la encuesta realizada entre los estudiantes de la materia de Seguridad de la información, nos encontramos que entre ellos existe conciencia acerca del valor que tienen las actividades de prevención de la pérdida de información y planificación de la recuperación ante desastres. Sin embargo, en su gran mayoría (cerca del 80%), admiten no poseer los conocimientos necesarios para realizar estas actividades, por lo que se debe ahondar en la preparación que deben adquirir en esta área. Un hallazgo de estas respuestas, que se considera interesante es que, hay un pequeño porcentaje (alrededor del 20%) de entre esos estudiantes encuestados, que afirma ser conocedor (incluso a nivel experto, cerca del 4%)) de estos servicios DRaaS, lo cual debe ser considerado cuando se estime que es necesario mejorar el nivel de conocimientos de los demás estudiantes.

Finalmente, la entrevista realizada, nos permitió conocer los servicios que actualmente están listos para ser entregados a la comunidad de estudiantes, profesores y personal administrativo de la Carrera de Software y los requerimientos de RPO y RTO para esos servicios

Propuesta

Se revisa la información de los servicios DRaaS ofrecidos por los proveedores AWS (Amazon Web Services), Microsoft Azure y Google Cloud Platform).

Los siguientes son diagramas representativos de las Arquitecturas de estos servicios

AWS

Servicio DRaaS. **AWS Elastic Disaster Recovery**

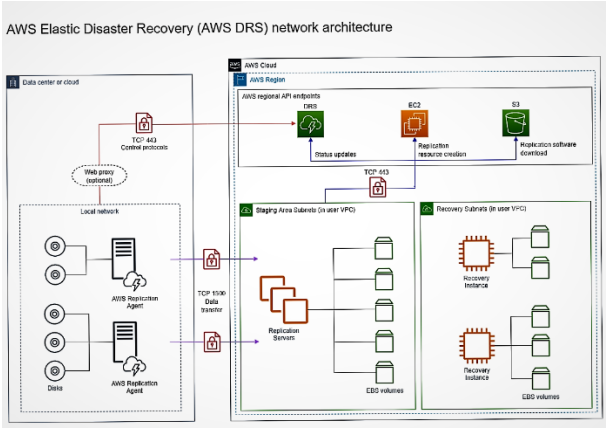

Figura 6 – Arquitectura AWS Elastic Disaster Recovery
Fuente: https://docs.aws.amazon.com/drs/latest/userguide/Network-diagrams.html

Microsoft AZURE

Servicio DRaaS. **Azure Site Recovery (ASR)**

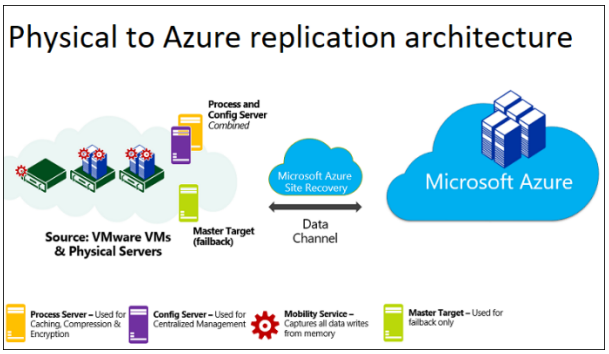

Figura 7 – Arquitectura Azure Site Recovery

Fuente:https://docs.microsoft.com/es-es/azure/site-recovery/physical-azure-architecture

Google Cloud Platform

Servicio DRaaS. **Actifio GO**

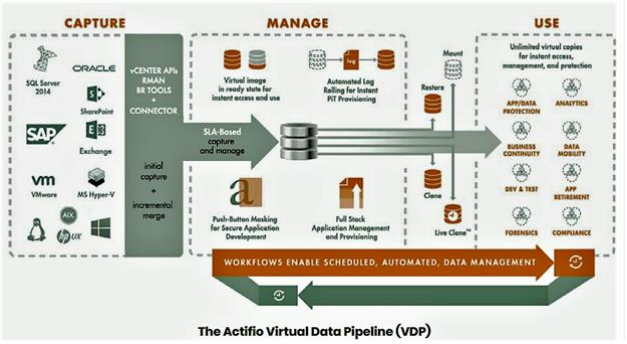

Figura 6 – Arquitectura Actifio GO

Fuente;https://docs.actifio.com/Actifio-GO/PDFs/Introducing.pdf

En este estudio, también se incluyó la realización de una encuesta a los estudiantes que estaban registrados en la materia Seguridad Informática y una entrevista al responsable de la Gestión del Centro de Datos de la Carrera de Software

Conclusiones

- Las soluciones DRaaS que ofrecen los tres proveedores, incluyen características tecnológicas y ventajas financieras y operativas que permiten superar las objeciones que, en nuestra región, siempre han enfrentado las implementaciones de los Planes de Recuperación ante Desastres. Se evita la necesidad de realizar las grandes inversiones y gastos que antes era necesario realizar, ya que se debía emplear un Centro de Datos Alterno,

con duplicación de equipos y que demandaban grandes esfuerzos para mantener la sincronización de las configuraciones y los datos.

- Desde el punto de vista operativo, los servicios en la nube presentan la ventaja de que el RPO se puede reducir a segundos y el RTO a minutos.
- Otra ventaja, es que, una vez que ya se cuentan con los primeros servidores y servicios configurados en el Servicio ofrecido por el proveedor de la nube, agregar otros servidores o servicios adicionales, es relativamente sencillo, Además, las pruebas de aseguramiento del buen funcionamiento de las recuperaciones configuradas o del Plan de Recuperación ante Desastres, se pueden realizar sin necesidad de interrumpir las operaciones de la empresa.
- Es importante destacar que estos tres proveedores cuentan con soluciones técnicamente diferentes entre sí, para atender la misma necesidad y que cada uno ofrece una arquitectura distinta. Microsoft ofrece una solución propia, que está disponible desde el año 2014, en tanto que Amazon y Google, ofrecen soluciones que fueron adquiridas a otras empresas. Este detalle que se ha mencionado, son hechos, que no se estiman que sean ventaja o desventaja relativa en la materia de este estudio, salvo quizá, la mayor experiencia y conocimiento interno que existe en Microsoft acerca de su servicio Azure Site Recovery
- En forma general, las tres soluciones cuentan con características funcionales .que se pueden considerar muy similares. En el proceso de la selección de la solución, es muy importante distinguir si el sistema operativo de la maquina original, esta soportada en todas y cada una de las soluciones DRaaS que se están examinando. También se deben identificar los eventuales requerimientos de servidores adicionales que tengan esas soluciones, ya que ellos podrían incrementar el costo de la solución y hacer más compleja su operación.
- Se realizó una prueba de concepto, empleando el Servicio Azure Site Recovery para proteger ante desastres, al Servidor de Active Directory. Esta prueba reviso los mecanismos de replicación de los datos de los servidores y de conmutación por error (Failover). La documentación de Microsoft Azure Site Recovery, indica que, para los servidores físicos (como el de Active Directory del Centro de Datos), no está soportada la conmutación por recuperación (Failback), hacia el servidor físico. Esta conmutación por recuperación, si se puede realizar, pero a una máquina virtual VMware. Esto conlleva la conclusión de que, la

realización de las pruebas de concepto de todas las soluciones a ser examinadas sea obligatoria, a fin de evitar resultados inesperados o tomar decisiones inconvenientes.

- Si no se realizan cambios en la infraestructura de los servidore de este Centro de Datos, no es posible concluir de manera objetiva, con un pronunciamiento acerca de cuál de los tres proveedores es el más conveniente para atender las necesidades de Recuperación de Servicios de esta unidad de la Carrera de Software.
- Si se realizan cambios (por ejemplo, que los servidores en funcionamiento sean virtuales con Hyper-V) es de esperarse que podamos contar con Azure Site Recovery como una solución aceptable para los objetivos de servicio de este Centro de Datos.
- Actualmente, la Universidad de Guayaquil, tiene un convenio con Microsoft para usar varios de los productos de la Plataforma Office 365 y que incluye el acceso al Portal de Azure, para toda la comunidad de nuestra Alma Mater. Con Azure se incluye el programa comercial dirigido al sector académico, denominado "Microsoft Azure Dev Tools for Teaching" el mismo que permite a los estudiantes y profesores, el uso de una serie de herramientas, programas y servicios, sin costo adicional

Recomendaciones

Luego de la realización de este estudio y de la prueba de concepto solicitada, es posible elaborar las siguientes recomendaciones:

- La selección del producto DRaaS más conveniente, debe incluir la revisión de las operaciones de configuración del producto para la replicación de los datos, la conmutación por error (Failover) y la conmutación por recuperación (Failback), ya que eso permitirá establecer las necesidades de otros equipos (servidores físicos o virtuales, almacenamiento, procesadores, memoria), software, redes, comunicaciones, seguridades. Adicionalmente, podremos conocer si es que las operaciones Failover y Failback, cumplen con las necesidades de servicio que tenga la empresa.
- Realizar una prueba de concepto, para asegurarse de que, las funciones ofrecidas, cumplen con las necesidades de respaldo y recuperación de los servicios.
- Realizar la implementación de un Plan de Recuperación ante Desastres, con la cantidad mínima de servicios que sea posible empezar, a fin de que se cumpla exitosamente con la curva de aprendizaje respectiva y se identifiquen los detalles de las operaciones del negocio,

de los procesos técnicos y administrativos que están relacionados con estas medidas que incrementan la resiliencia. Luego, con la experiencia adquirida, se pueden incluir los demás servicios ofrecidos, en la secuencia que establezca el análisis de riesgos que se haya realizado.

- Cuando haya mayor conocimiento y experiencia en esta materia, buscar la reducción de los RTO comprometidos, aplicando la mayor automatización de los procesos de recuperación que sea posible,
- Realizar, de manera planificada, la realización de las pruebas de los planes de recuperación, con la periodicidad que permita asegurar que los planes si funcionan correctamente y que el personal conserva las destrezas para actuar cuando llegue el momento de emplear los recursos de recuperación definidos e implementados.
- Incorporar indicadores de Disponibilidad en el control de las actividades del Centro de Datos, que permitan ver la evolución que están teniendo los servicios de tecnología que está entregando.
- Hacer el mayor esfuerzo posible, para que la implementación de los servicios tecnológicos, en el Centro de Datos de la carrera de Software, se realice empleando la tecnología de la virtualización, ya que ellos cuentan con servicios de recuperación mucho más flexibles y eficientes, que los que se ofrecen a los servidores físicos.

Referencias

1. Aldea, A., Vaicekauskaitė, E., Daneva, M., & Piest, J. (2021). Enterprise Architecture Resilience by Design: A Method and Case Study Demonstration. 2021 IEEE 25th International Enterprise Distributed Object Computing Workshop (EDOCW) (págs. 147-156). Gold Coast, Australia: IEEE. doi:10.1109/EDOCW52865.2021.00044
2. Arnal Zaragozá, D. (25 de 09 de 2020). Linkedin. Recuperado el 26 de Julio de 2022, de ¿Tu copia de seguridad protege el negocio?: https://es.linkedin.com/pulse/tu-copia-de-seguridad-protege-el-negocio-daniel-arnal-zaragoz%C3%A1
3. AXELOS Limited. (2019). ITIL Foundation: ITIL 4 edition. (Primera ed.). London, England: Norwich, TSO (The Stationery Office). Recuperado el 26 de 07 de 2022

4. Brende, B., & Sternfels, B. (20 de Mayo de 2022). https://www.mckinsey.com/. (W. E. Forum, Ed.) Recuperado el 10 de Julio de 2022, de https://www.weforum.org/whitepapers/resilience-for-sustainable-inclusive-growth/: https://www.mckinsey.com/~/media/mckinsey/business%20functions/risk/our%20insights/resilience%20for%20sustainable%20inclusive%20growth/resilience-for-sustainable-inclusive-growth_final.pdf?shouldIndex=false
5. Crask, J. (2021). Business Continuity Management: A Practical Guide to Organizational Resilience and ISO 22301 1st Edición (Primera ed.). London, United Kingdom: Kogan Page. Recuperado el 13 de 07 de 2022
6. Gibbs, L., Jehangir, H., Leung Kwong, E. J., & Little, A. (24 de Junio de 2022). Universities and multiple disaster scenarios: A transformative framework for disaster resilient universities. International Journal of Disaster Risk Reduction, 78(103132), 9. doi:https://doi.org/10.1016/j.ijdrr.2022.103132
7. International Organization for Standardization. (02 de 2021). Security and resilience — Vocabulary. ISO 22300:2021, Tercera, 53. Geneva, Switzerland. Recuperado el 24 de Julio de 2022, de Online Browsing Platform (OBP): https://www.iso.org/obp/ui/#iso:std:iso:22300:ed-3:v1:en
8. International Organization for Standardization;. (02 de 2022). Information security, cybersecurity and privacy protection — Information security controls. ISO/IEC 27002:2022, Tercera, 152. Geneva, Switzerland. Recuperado el 25 de 07 de 2022, de https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-3:v2:en
9. Revista Datacenter. (12 de 12 de 2013). Revista Datacenter. Recuperado el 25 de Julio de 2022, de ¿RTO vs RPO?: https://revistadatacenter.wordpress.com/2013/12/12/cual-es-la-diferencia-entre-el-rto-y-rpo/
10. Ruiz-Martin, C., López-Paredes, A., & Wainer, G. (31 de 01 de 2018). What we know and do not know about organizational resilience. (Prof. Eduardo Vicéns-Salort, Ed.) International Journal of Production Management and Engineering, 6(1), 11-28. doi:10.4995/ijpme.2018.7898
11. Sanchis, R., & Poler, R. (12 de 2020). Resiliencia Empresarial en Época de Pandemia. Boletín de Estudios Económicos, 75(231), 501-520. Recuperado el 11 de Julio de 2022, de https://riunet.upv.es/handle/10251/165594

12. Sarkar, A., Wingreen, S. C., & Cragg, P. (2013). Organisational IS Resilience: a pilot study using Q-methodology. ACIS 2013: Information systems: Transforming the Future: Proceedings of the 24th Australasian (págs. 1-11). Melbourne, Australia: RMIT University. Recuperado el 10 de Julio de 2022, de https://aisel.aisnet.org/acis2013/134
13. Terinte, T. (26 de 06 de 2018). Effects of Cloud Computing on Enterprises. Master's thesis, Masaryk University, Faculty of Economics and Administration, Brno. Recuperado el 27 de Julio de 2022, de https://is.muni.cz/th/rc7xo/?predmet=674645;lang=en;id=234077
14. Wolbers, J., Kuipers, S., & Boin, A. (2021). A systematic review of 20 years of crisis and disaster research: Trends and progress. Risk, Hazards, & Crisis in Public Policy (RHCPP), 12(4), 374–392. doi:10.1002/rhc3.12244