UNIVERSIDAD DON BOSCO

VICERRECTORÍA DE ESTUDIOS DE POSTGRADO

TRABAJO DE GRADUACIÓN

ANÁLISIS PARA IMPLEMENTACIÓN DE PLAN DE RECUPERACIÓN DE DESASTRES (DRP) EN LA NUBE PÚBLICA PARA INSTITUCIONES EDUCATIVAS PRIVADAS CLASIFICADAS COMO PEQUEÑA O MEDIANA EMPRESA.

PARA OPTAR AL GRADO DE MAESTRO EN SEGURIDAD Y GESTIÓN DE RIESGOS INFORMÁTICOS

ASESOR:

RUDIGER FOGELBACH FIGUEROA

PRESENTADO POR:

SALVADOR EDUARDO AMAYA GÓMEZ

FRANCISCO ALBERTO CUERNO MAGAÑA

MANUEL ALEJANDRO SILIEZAR DURAN

Antiguo Cuscatlán, La Libertad, El Salvador, Centroamérica

Julio de 2018

AGRADECIMIENTOS

“A mi Dios, y a mi familia que es la presencia de él en mi vida "

Salvador

“A Dios sobre todas las cosas, a mi familia y a mi madre que siempre han estado a mi lado apoyando mis sueños.”

Francisco

RESUMEN

Con el presente análisis se pretende aportar referencias y lineamientos a las instituciones educativas del sector privado la forma adecuada para la implementación de un plan ante desastres, utilizando los servicios de la nube, en caso de catástrofes naturales o humanas, para reducir el riesgo de pérdida de información que afecten los servicios académicos actuales y presentarles una guía de trabajo para estar preparados ante un evento

El análisis fue realizado tomando en consideración aquellas instituciones educativas que estén en la clasificación como pequeña o mediana empresa; que cuenten o no con una infraestructura tecnológica en sus centros educativos; ya sea por costos de mantenimiento o recurso humano.

Tener un plan de continuidad del negocio para clasificar todos aquellos servicios críticos que pueden afectar a la institución teniendo alguna consecuencia que pueda afectar su capacidad económica y/o su reputación. Para esto se presenta dentro del análisis la norma ISO 22301 sobre "Gestión de continuidad del negocio".

Luego de haber clasificado cada uno de sus servicios más críticos, dentro del presente documento se presentan información de 3 grandes proveedores de servicios en la nube como lo son Microsoft con su plataforma Azure, Google Plataform y VMware Cloud; los mayores proveedores de servicios en la actualidad.

Antes de seleccionar a algún proveedor de servicios en la nube y evaluar todos aquellos servicios críticos de la institución se debe hacer un análisis para la implementación de un DRP en la nube.

Los resultados que puedan presentarse durante el análisis en estas instituciones nos darán a conocer que tan preparadas están en caso del algún evento catastrófico.

ÍNDICE

Lista de Figuras

Lista de tablas

Lista de Graficas

I. INTRODUCCIÓN

Las razones por las cuales se está desarrollando el presente trabajo de investigación, es para conocer si las instituciones educativas conocen los servicios de la nube, saber qué servicio actualmente tienen contratados y para que lo utilizan.

Adicionalmente se busca analizar a las instituciones educativas del sector privado, conocer su clasificación como empresa, saber si están preparados en caso de alguna catástrofe natural o humana para restablecer sus servicios y si tienen un plan de continuidad de negocio en caso ocurra.

El objeto principal del análisis para la implementación de un DRP en la nube es saber que tecnológicas en la nube utilizan, si las conocen a profundidad, y si conocen los tipos de servicios de los cuales han adquirido y en que clasificación de servicio se encuentran.

Específicamente se pretende:

- Encuestar determinadas instituciones educativas para conocer los servicios que utilizan, tamaño de infraestructura, como se clasifican por tamaño de empresa, entre otras, para lograr analizar esta información y proponer lineamientos para la implementación de un plan de recuperación en caso de desastres (DRP).
- Seguir lineamientos de la ISO 22301 “Continuidad del negocio” como una guía en casos de eventos naturales o humanos.
- Conocer sus procesos más críticos y analizar los tiempos de respuesta para su recuperación (RTO) y restablecer sus servicios en algún punto en el tiempo (RPO).
- Presentar los servicios de recuperación ante desastres como una opción más a los servicios que actualmente utilizan.
- Brindar la información adecuada sobre los proveedores de servicios en la nube, que actualmente ofrecen este servicio (Microsoft Azure, Google Platform, VMware Cloud).
- Brindar las bases de conocimiento necesarias para tener un plan de recuperación ante desastre utilizando los servicios de la nube.

El presente documento ha sido elaborado con un enfoque metodológico basado en la investigación bibliográfica, documentación técnica relacionada y una encuesta en línea a diez (10) instituciones educativas del sector privado del área metropolitana.

El documento está articulado de manera; que por ser un análisis para la implementación de un plan de recuperación ante desastres (DRP), sea una guía que brinde los pasos adecuados para que la información de las instituciones educativas del sector privado este siempre disponible en caso de desastres.

II. MARCO TEORICO

El marco teórico que fundamenta esta investigación proporciona al lector una idea más clara de cómo implementar un plan de recuperación ante desastres (DRP) en las instituciones educativas del sector privado. Expone mucho los conceptos de los distintos servicios de la nube, los tipos infraestructura en la nube, los servicios que cada proveedor ofrece y por su ende, el análisis para la implementación del plan de recuperación utilizando distintas herramientas, tanto tecnológicas como procedimentales (ISO 22301, Proveedores de Servicios en la nube).

2.1 CLASIFICACION DE LAS PYMES DEL SECTOR EDUCATIVO

La abreviación PYME se utiliza con frecuencia para denominar las pequeñas y medianas empresas en la Unión Europea [1] y las organizaciones internacionales tales como el Banco Mundial, las Naciones Unidas y la Organización Mundial del Comercio. [2]

El Salvador como miembro de las Naciones Unidas, ha tomado como referencia la clasificación utilizada, con lo que da paso a la Ley de Fomento, Protección y Desarrollo para la Micro y Pequeña Empresa que fue aprobada por la Asamblea Legislativa el 25 de abril del 2014 y entró en vigor el 28 de mayo del 2014. Esta ley es producto de un proceso participativo que incluyó consultas que CONAMYPE (Comisión Nacional de la Micro y Pequeña Empresa) lideró desde el año 2010.

La ley en donde legalmente se clasifica si es micro o pequeña empresa dice así: [3]

Art. 3.- Las Micro y Pequeña Empresa estarán clasificadas de la siguiente manera:

a) Microempresa: Persona natural o jurídica que opera en los diversos sectores de la economía, a través de una unidad económica con un nivel de ventas brutas anuales hasta 482 salarios mínimos mensuales de mayor cuantía y hasta 10 trabajadores.

b) Pequeña Empresa: Persona natural o jurídica que opera en los diversos sectores de la economía, a través de una unidad económica con un nivel de ventas brutas anuales mayores a 482 y hasta 4,817 salarios mínimos mensuales de mayor cuantía y con un máximo de 50 trabajadores.

Categoría de empresa	Número de Empleados
Mediana	Mayor 50
Pequeña	Menor 50
Micro	Hasta 10

Tabla 1 - categorías de empresas según número de empleados [13]

Con base a la clasificación, y a la importancia que las PYMES representan a la economía de El Salvador al representar cerca del 99% del sector empresarial del país, con lo que contribuye al sostenimiento y crecimiento de la economía nacional. Estimando que las MYPE generan aproximadamente 700 mil empleos directos y aportan alrededor del 35% del Producto Interno Bruto (PIB) y en conjunto consumen más insumos y servicios que las grandes empresas. [3]

2.2 DESCRIPCION DE LAS INSTITUCIONES EDUCATIVAS SEGÚN SU CLASIFICACION

2.2.1 Clasificación de Colegio San Francisco

Nombre de la Institución	**Colegio San Francisco**
Inicio de Operaciones	**1977**
Clasificación PYME	**Mediana Empresa**
No de Empleados	**Mayor 50**

Tabla 2 - Información Colegio San Francisco

2.2.2 Clasificación de Colegio Americano

Nombre de la Institución	**Colegio Americano**
Inicio de Operaciones	**2005**
Clasificación PYME	**Mediana Empresa**
No de Empleados	**Mayor 50**

Tabla 3 - Información Colegio Americano

2.2.3 Clasificación de Colegio “A Child for Christ”

Nombre de la Institución	**Colegio Cristiano Bilingüe “A Child for Christ”**
Inicio de Operaciones	**1987**
Clasificación PYME	**Pequeña Empresa**
No de Empleados	**Mayor 10 menor 50**

Tabla 4 - Información Colegio Cristiano Bilingüe "A child for Christ"

2.2.4 Clasificación de Colegio Ricaldone

Nombre de la Institución	**Colegio Ricaldone**
Inicio de Operaciones	**1957**
Clasificación PYME	**Mediana Empresa**
No de Empleados	**Mayor 50**

Tabla 5 - Información Colegio Ricaldone

2.2.5 Clasificación de Universidad Don Bosco

Nombre de la Institución	Universidad Don Bosco
Inicio de Operaciones	1980
Clasificación PYME	Mediana Empresa
No de Empleados	Mayor 50

Tabla 6 - Información Universidad Don Bosco

2.2.6 Clasificación de Universidad Francisco Gavidia

Nombre de la Institución	Universidad Francisco Gavidia
Inicio de Operaciones	1955
Clasificación PYME	Según la cantidad de empleados dada por la institución, sobrepasa el criterio de PYME, pero lo dejaremos en el listado por la información obtenida de los conocimientos y usos de la nube.
No de Empleados	Mas de 1,000

Tabla 7 - Información Universidad Francisco Gavidia

2.3 NORMA ISO 22301 – GESTIÓN DE CONTINUIDAD DEL NEGOCIO

Actualmente las empresas se orientan en la ISO 22301 para diseñar sus estrategias de gestión de continuidad de negocios, mencionaremos de una forma general que es esta norma, como guía para entender cómo se hace un plan de continuidad de negocio estructurado.

La ISO 22301 es una norma internacional de gestión de continuidad de negocio. Esta identifica los fundamentos de un Sistema de Gestión de la Continuidad de Negocio (SGCN), estableciendo el proceso, los principios y la terminología de gestión de continuidad de negocio.

Proporciona una base de entendimiento, desarrollo e implantación de continuidad de negocio dentro de la organización. Se usa para asegurar a las partes interesadas que su empresa está totalmente preparada y que puede cumplir con los requisitos internos, regulatorios y del cliente.

La norma proporciona a las organizaciones un marco de referencia que asegura que ellos pueden continuar trabajando durante las circunstancias más difíciles e inesperadas, siempre protegiendo a sus empleados, manteniendo su reputación y proporcionando la capacidad de continuar trabajando y ofreciendo sus servicios.

La norma ISO 22301 puede ser aplicada a todo tipo y tamaño de organizaciones que necesiten:

● Establecer, implantar, mantener y mejorar un SGCN.

● Demostrar conformidad con la política establecida de la continuidad de negocio de la organización.

● Dar a las partes interesadas confianza en su conformidad y compromiso con las buenas prácticas reconocidas internacionalmente.

2.3.1 Estructura de la norma ISO 22301

La norma ISO 22301 está organizada según la siguiente estructura:

1. Ámbito de aplicación.
2. Referencias normativas.
3. Términos y definiciones.
4. Contexto de la organización. Consiste en identificar el alcance del SGCN, teniendo en cuenta los objetivos estratégicos de la organización, sus productos y servicios claves, su tolerancia al riesgo, así como cualquier obligación reglamentaria.
5. Liderazgo. La alta dirección debe demostrar un compromiso continuo con el SGCN. A través de su liderazgo y acciones, la dirección puede crear un ambiente en el cual el personal esté completamente involucrado y el sistema de gestión pueda funcionar de manera eficaz en sinergia con los objetivos de la organización.
6. Planificación. Se establecen objetivos estratégicos y principios para la orientación del SGCN en su totalidad.
7. Soporte. La gestión diaria de un Sistema de Gestión de la Continuidad de Negocio se basa en el uso de los recursos apropiados para cada actividad. Estos recursos incluyen personal competente, toma de conciencia y comunicación, etc. todo esto debe estar apoyado por la documentación que sea necesaria.
8. Operación. Después de la planificación del SGCN, la organización debe ponerlo en funcionamiento.
9. Evaluación del desempeño. La norma ISO 22301 requiere un seguimiento permanente del sistema, así como revisiones periódicas para mejorar su operación. [4]
10. Mejora. La organización puede mejorar continuamente la eficacia de su sistema de gestión a través del uso de la política de continuidad de negocio, los objetivos, los resultados de

auditorías, los indicadores, las acciones correctivas y preventivas y la revisión por la dirección.

Esta estructura de la norma está basada en el modelo de mejora continua, conocida como ciclo Deming que en español se conoce como ciclo PHVA (Planificar-Hacer-Verificar-Actuar).

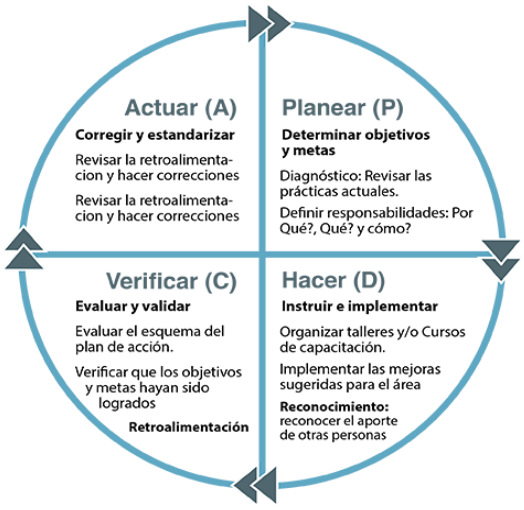


Figura 1 - Ciclo de mejora continua de Deming

Los principales puntos que podemos proteger gracias al Sistema de Gestión de Continuidad de Negocio son:

- Recuperación ante interrupciones imprevistas.
- Posibles bloqueos económicos o legales.
- Daños en la reputación y las responsabilidades.

Una vez se establecen todos los objetivos de la política de continuidad de negocio, no sólo debemos tener en cuenta la protección de las aplicaciones, los datos y los servicios según la empresa utilizando una amplia gama de amenazas, sino que tenemos que evaluar otros aspectos prácticos a tener en cuenta como pueden ser:

- Limitaciones en el presupuesto. (punto importante para las PYMES)
- Limitaciones en personal.

2.3.2 ISO 22301 para pequeñas y medianas empresas (PYMES)

No solamente las grandes organizaciones pueden resultar afectadas por perturbaciones inesperadas. Las pequeñas y medianas empresas también enfrentan amenazas similares.

Sin importar el tamaño de su organización, hoy en día, la capacidad de responder eficientemente es más crítica que nunca. Es por eso por lo que los sistemas de gestión de continuidad del negocio ISO 22301 se diseñaron para ayudarle a gestionar los riesgos que amenazan la operación de las empresas sin contratiempos y garantizar su supervivencia en el caso de una perturbación.

Las empresas pequeñas y medianas que implementan ISO 22301 pueden mejorar su fiabilidad de la misma manera que las organizaciones grandes [11]. Se presume que las PYMES tienen presupuestos bajos y disponen de menos tiempos para implementar un sistema de gestión de continuidad de negocios, pero eso no es limitante para su desarrollo utilizando la norma ISO 22301 como guía, y utilizando recursos tecnológicos como los encontrados en la nube computacional (concepto tecnológico que se explicará más adelante en este documento).

Con el paso de los años, cada organización tiene la necesidad de ir creciendo con la ayuda de la tecnología, mejorando el procesamiento y uso de la información. Sin embargo, ante una contingencia, donde ocasionará la pérdida de datos en una organización:

Eventos por la naturaleza:

- Huracanes
- Inundaciones
- Terremotos
- Incendios
- Explosiones

Al presentarse alguno de ellos pueden traer consigo la interrupción de los servicios por falta de electricidad, comunicaciones, etc.

Eventos por el hombre:

- Sabotaje
- Fraude
- Ataques terroristas
- Ataques maliciosos, etc.

Al presentarse alguno de ellos pueden traer consigo la pérdida de la información, de la confiabilidad, desviación de fondos, falsificación de datos, errores en la información, caídas en el servicio, etc. [12].

Estadísticas que debemos tener presente, nos mencionan lo siguiente [5]:

- 6% las computadoras sufren algún evento de pérdida de datos en cualquier año.

- 30% de todas las empresas que tienen un gran incendio se queden fuera del mercado hasta un año.
- El 31% de los usuarios de computadoras han perdido todos sus archivos debido a eventos fuera de su control.
- 34% de las empresas no logran probar sus copias de seguridad en cinta, y de las que sí lo hacen, el 77% han encontrado problemas en éstas.
- 60% de las empresas que pierden sus datos cerrarán dentro de los siguientes 6 meses después del desastre.
- Las empresas que no son capaces de reanudar sus operaciones dentro de los diez días siguientes de un desastre, no es probable que sobrevivan.
- Cada semana 140,000 discos duros dejan de funcionar en los Estados Unidos.

Fuente: Boston Computing Network (1998).

Las anteriores estadísticas nos muestran que somos muy susceptibles a perder datos y/o servicios críticos y/o importantes si no tomamos las medidas de protección pertinentes. Para reducir estos eventos y controlarlos hasta cierto grado, se hace necesario el desarrollar estrategias para proteger nuestra información y servicios mediante un plan de recuperación ante desastre (*DRP - Disaster Recovery Plan*). [5]

2.4 CONTINUIDAD DEL NEGOCIO Y PLAN DE RECUPERACION ANTE DESASTRES

El plan de recuperación ante desastres (*DRP - Disaster Recovery Plan*) y el plan de continuidad del negocio (*BCP - Business Continuity Plan*) están diseñados ante un eventual desastre con el sistema informático. Para una contingencia del sistema informático, es necesario garantizar la protección de los datos. El desarrollo de estos planes, le permitirá anticipar los riesgos a los que está expuesto su sistema informático en caso de desastres.

El plan de recuperación le permite conocer el equipo y el rol de cada uno de los que están a cargo del plan de recuperación, así como la lista de procedimientos a seguir.

El Plan de continuidad del negocio (*BCP*) es el último eslabón de la cadena y se aplica únicamente para proteger las aplicaciones que son vitales para la actividad de la empresa.

Los beneficios que trae consigo un *BCP* en una organización son:

- Minimiza las potenciales pérdidas económicas que pueden derivar de un Incidente de Seguridad no analizado.
- Reduce los riesgos potenciales de la Organización, a través del análisis de impacto.
- Reduce significativamente las interrupciones de los Servicios.
- Asegura la estabilidad de la Organización y sus clientes.
- Protege los activos de Información.
- Minimiza el riesgo de tomas de decisiones erradas durante el acontecimiento de un evento.
- Minimiza las responsabilidades legales.

Algunos de los beneficios que podrá gozar una organización al hacer un DRP, a parte de los ahorros del esfuerzo, tiempo y dinero:

- Mantener la continuidad de los servicios relacionados con las tecnologías de información (TI) del negocio:
- Proteger al negocio de fallas generales en los servicios informáticos.
- Minimizar los riesgos generados por la falta de servicios.
- Garantizar el acceso de la información empresarial.
- Mantener la disponibilidad de los recursos informáticos.
- Minimizar la toma de decisiones erróneas al presentarse algún desastre.
- Dar atención continua a los clientes, proveedores, accionistas, colaboradores.
- Tener capacidad de recuperación exitosa.

La recuperación ante desastres se enfoca en el restablecimiento de los sistemas e infraestructura de TI que soportan los procesos de negocio críticos después de eventos de interrupción, mientras que la continuidad del negocio está orientada a la recuperación de los procesos de negocio críticos que son necesarios para la operación, por lo que no solo incluye lo anterior, sino también todos los demás aspectos operativos necesarios dentro de la organización. El DRP es un eslabón importante dentro del plan de continuidad del negocio, tal como se muestra en la siguiente figura:

Figura 2 - Plan de continuidad del negocio [14]

El DRP es un plan que indica las acciones que se deben realizar en un período de tiempo especificado en los casos de que alguna contingencia (siniestro, desastre) imposibilite el funcionamiento de los recursos informáticos en forma parcial o total de una organización. El DRP permite recuperar los servicios críticos de la organización.

Por tanto, es obligación de éste el controlar los efectos que pudieran producir los desastres, es decir, cada uno del personal debe comprometerse a minimizar y administrar los riesgos que pudieran generar los desastres informáticos.

El DRP se debe aplicar:

- Antes de que ocurra una contingencia.
- Durante la ocurrencia de la contingencia.
- Después de que ocurra la contingencia.

2.4.1 Plan Tradicional de recuperación ante Desastres

Los planes de recuperación de desastres (DRP) son una declaración exhaustiva de las acciones que deben tomarse antes, durante y después de que un evento perturbador cause la pérdida de disponibilidad de los sistemas de información. El objetivo principal es proporcionar un sitio de procesamiento alternativo y regresar al sitio primario dentro de un marco de tiempo mínimo cuando ocurra cualquier desastre en los sistemas de información. [6]

En un evento de desastre, una compañía con un DRP debe ser capaz de garantizar adecuadamente las siguientes actividades:

- Cambiarse al sitio DRP
- Cambio de los enlaces de red del sitio afectado al sitio de recuperación de desastres
- Asegurar los enlaces de red del sitio de recuperación.
- Restaurar los sistemas de respaldo (servidores).
- Restaurar datos asegurando su integridad.
- Verificar la disponibilidad del sistema y los datos a través de la red.
- Restaurar las aplicaciones.
- Verificando la disponibilidad funcional del sistema de información.
- Rehacer el sistema de información a los usuarios.

Estas acciones deben planificarse de acuerdo con dos requisitos de tiempo definidos en una entrevista realizada a los usuarios del sistema de información:

RTO (Recovery Time Objective): La duración específica del tiempo en que las funciones comerciales no están disponibles

RPO (Recovery Point Objective): El período de tiempo máximo entre dos copias de seguridad sucesivas, y, por lo tanto, la cantidad máxima de datos que se puede perder debido a un incidente importante cuando la restauración es exitosa.

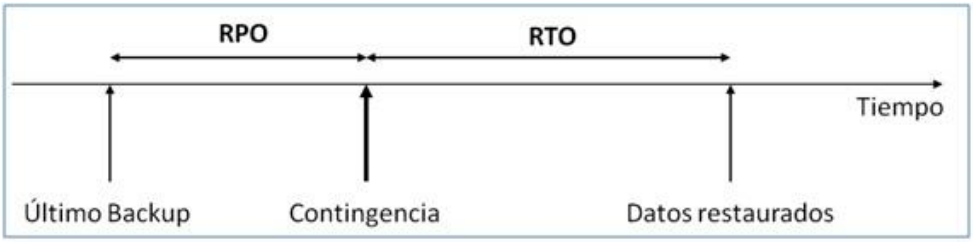


Figura 3 - Recuperación de desastres RPO y RTO [25]

Un concepto clave en un DRP es la separación geográfica de los sitios primario y de respaldo. Una fracción significativa de los desastres, incluidos los causados por interrupciones, son geográficos en la naturaleza como se muestra en la Tabla 8, que da esa porción de organizaciones que han enfrentado desastres durante los últimos cinco años
Cuando el procesamiento de las transacciones es cambiado desde el sitio primario (en estado de falla) al sitio de respaldo, a este cambio se le denomina *failover* (cambio por fallo). Cuando las causas de la falla primaria se han solventado y el cambio se realiza de nuevo al sitio primario, este cambio se le denomina se denomina *failback* (cambio por recuperación). Varias opciones surgen dependiendo de la naturaleza del sitio de respaldo y cómo se relaciona al proceso en el sitio primario.

Causas	Organizaciones
Actualización de Sistemas	72%
Interrupción/Fallas de energía	70%
Incendio	69%
Administración de cambios	64%
Ataques Cibernéticos	63%
Empleados malintencionados	63%
Pérdida/daño de la información	63%
Inundación	48%
Huracán	46%
Terremoto	46%
Tornado	46%
Terrorismo	45%
Tsunami	44%
Erupción de volcanes	42%
Guerras	42%
Otros	1%

Tabla 8 -Causas de desastres que han generado un DRP [21]

2.4.2 Estrategias Tradicionales de recuperación de desastres

Para respaldar el sitio principal, las empresas generalmente usan un segundo sitio físico propio, con un segundo centro de cómputo o se contrata un centro de cómputo externo a un proveedor. Este segundo sitio se puede clasificar según el nivel de emergencia:

- **Sitio caliente (*hot site*):** es un centro de cómputo remoto que es redundante y completamente igual con el sitio primario.
- **Sitio Tibio (*warm site*)**: es un centro de cómputo remoto que es parcialmente equipado con equipos informáticos.
- **Sitio frío (*cold site*):** es un centro de cómputo remoto, disponible a partir de la activación del DRP no tiene ningún equipo previamente instalado. Entonces es necesario suministrar todo el equipo en caso de desastre.

Una vez que se establece el tipo de sitio de recuperación de desastres, deben de ser enviados los datos necesarios a través de diversas técnicas:

- Replicación asincrónica de un sistema a otro a través de una red IP.
- Replicación sincrónica de un arreglo de discos a otro arreglo, a través de un área de almacenamiento.
- Envío de cintas de copia de seguridad al sitio de recuperación de desastres a través de un medio de transporte.

2.4.3 Aspectos negativos de las estrategias tradicionales de DRP.

En general, una empresa debe planificar su estrategia de recuperación ante desastres de acuerdo con un bajo RTO y RPO. Esta condición hace que las empresas utilicen el método convencional de *DRP* usando la estrategia de (*hot site) o (warm site).* En estas estrategias la infraestructura está dedicada a una sola empresa. Este tipo de solución permite un tiempo de recuperación más corto en comparación con otros modelos convencionales como él (*cold site)*; es decir, la infraestructura de TI está replicada en el sitio de recuperación y listo para ser activado en el caso de desastre. Esta estrategia es costosa porque el equipo no se usa en condiciones normales. Algunas empresas usan su infraestructura de respaldo para el propósito de las pruebas y el desarrollo para compensar los costos, pero esto introduce un riesgo adicional de reconfiguración en caso de necesitarse en el plan. Finalmente, el proceso de restaurar los datos genera una incertidumbre en el proceso. La recuperación de datos puede demorar horas, incluido lapsos de tiempo de recuperación, transporte y carga de los datos. En un modelo compartido, la infraestructura se agrupa entre varias empresas. Eso se supone que es más barato porque la recuperación de desastres se comparte entre varias empresas.
En caso de un incidente, los equipos, el sistema operativo y aplicaciones en el sitio de recuperación de desastres debe estar completamente configurado para que coincida con el sitio principal dañado. Este proceso puede tomar varias horas o incluso días.

Además, las empresas que desarrollan e implementan un DRP, enfrenta los siguientes problemas:

- Dificultad para identificar los servidores que deben estar en el DRP.
- La complejidad de las soluciones técnicas internas o externas para implementar el DRP.
- El movimiento de recursos más hábiles para operar el DRP.
- La complejidad y el costo para mantener, en el tiempo, la infraestructura de los dos sitios (primaria y desastre) a un mismo nivel.
- La dificultad en el desarrollo de la recuperación de desastres soluciones en términos de requisitos comerciales.
- La incapacidad de organizar pruebas regulares de rescate.

Estos aspectos mencionados anteriormente, hacen que las estrategias tradicionales de recuperación ante desastres a menudo están fuera del alcance de las PYME, principalmente por razones financieras y complejidad.

	Método Tradicional	**Servicio en la Nube**
Renovación de recursos cada cierto tiempo para que no se vuelvan obsoletos	Si	No
Mantenimiento de hardware para que sigan funcionando correctamente	Si	No
Almacenamiento externo para los datos	Si	Si
Mantenimiento Energía Eléctrica - UPS	Si	No
Cableado estructurado	Si	No
Equipo Firewall	Si	No
Conectividad con el sitio principal	Si	Si
Licenciamiento de Sistema Operativo	Si	No
Respaldos en tiempo real y llevarlos fuera del servidor	No	Si
Replicación de base de datos en tiempo real	Si	Si
Replicación de información	Si	Si
Sistemas ya preinstalados	No	Si

Tabla 9 - Comparativa DRP vs DRaaS

2.5 MODELOS Y SERVICIOS DE LA NUBE

2.5.1 Que es la computación en la nube

"Viene desde los primeros días de Internet donde dibujamos la red como una nube... no nos importaba a dónde iban los mensajes... la nube no nos dejaba ver " [7]

Se puede decir que la primera nube en las redes fue el uso del protocolo TCP/IP. La segunda nube por lo tanto es el uso y administración de documentos en la WWW (World Wide Web).

La función de la nube como concepto emergente en nuestros días, combina las complejidades de infraestructura de servidores, aplicaciones, datos y plataformas heterogéneas.

Se usará el concepto de nube computacional que proporciona NIST (National Institute of Standards and Technology) que es la responsable de desarrollar estándares y directrices, incluidos los requisitos mínimos de dichos estándares para proporcionar seguridad de información adecuada para todas las operaciones y activos de la agencia; pero tales estándares y directrices no se aplicarán a los sistemas de seguridad nacional.

La computación en la nube es un modelo para permitir el acceso conveniente y bajo demanda a una red compartida con recursos informáticos configurables (ejemplo: redes, servidores, almacenamiento, aplicaciones y servicios) que puede aprovisionarse y liberarse rápidamente con un mínimo esfuerzo de gestión o interacción del proveedor de servicios.

Figura 4 - Computación en la nube [17]

2.5.2 Modelos de la computación en la nube

Private Cloud: La infraestructura de la nube se aprovisiona para uso exclusivo de una única organización que comprende múltiples consumidores (por ejemplo, unidades de negocio). Puede ser propiedad, administrado y operado por la organización, un tercero o una combinación de ellos, y puede existir dentro o fuera de las instalaciones [13].

Community Cloud: La infraestructura en la nube se aprovisiona para uso exclusivo de una comunidad específica de consumidores de organizaciones que han compartido inquietudes (por ejemplo, misión, requisitos de seguridad, política y consideraciones de cumplimiento).

Puede ser propiedad, administrado y operado por una o más de las organizaciones en la comunidad, un tercero o una combinación de ellas, y puede existir dentro o fuera de las instalaciones [13].

Public Cloud: La infraestructura de la nube está provista para uso abierto por el público en general. Puede ser propiedad, administrado y operado por una organización empresarial, académica o gubernamental, o alguna combinación de ellos. Existe en las instalaciones del proveedor de la nube [13].

Hybrid Cloud: La infraestructura de nube es una composición de dos o más infraestructuras de nube distintas (privadas, comunitarias o públicas) que permanecen como entidades únicas, pero están unidas por tecnología estandarizada o patentada que permite la portabilidad de datos y aplicaciones (por ejemplo, ruptura de nubes para equilibrio de carga entre nubes) [13].

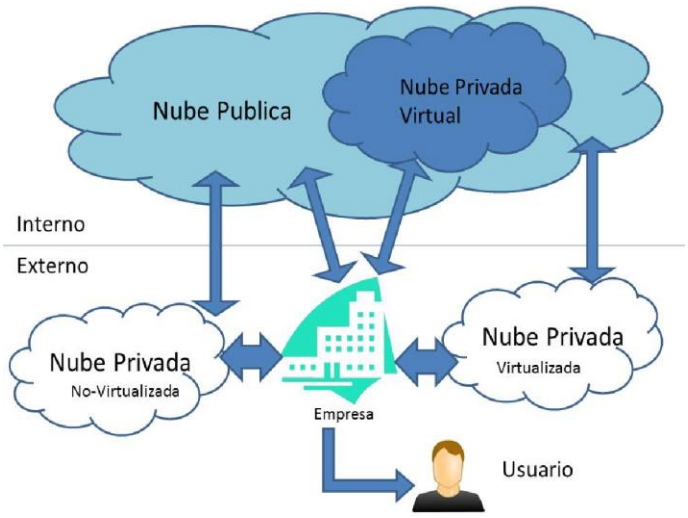


Figura 5 - Modelos de nubes computacionales [16]

2.5.3 Servicios de la computación en la nube

Actualmente los servicios de la nube se pueden visualizar en sus 3 principales servicios que fueron los primeros servicios creados antes que estos mismos se fueran expandiendo en otros microservicios para tratar de ayudar a las compañías a ahorrar costos y no adquirir los paquetes completos de estos servicios:

***Infrastructure as a Service* (IaaS):** La capacidad provista al consumidor es proporcionar procesamiento, almacenamiento, redes y otros recursos informáticos fundamentales donde el consumidor puede implementar y ejecutar software arbitrario, que puede incluir operaciones sistemas y aplicaciones. El usuario no administra ni controla la nube subyacente infraestructura, pero tiene control sobre los sistemas operativos, el almacenamiento y las aplicaciones implementadas; y posiblemente un control limitado de los componentes de red seleccionados (por ejemplo, firewalls host) [13].

***Software as a Service* (SaaS):** La capacidad provista al consumidor es usar el proveedor aplicaciones que se ejecutan en una infraestructura de nube. Las aplicaciones son accesibles desde varios dispositivos cliente a través de una interfaz de cliente ligero, como un navegador web (por ejemplo, correo electrónico basado en web), o una interfaz de programa. El consumidor no administra ni controla el Infraestructura de nube subyacente que incluye red, servidores, sistemas operativos, almacenamiento o incluso capacidades de aplicación individuales, con la posible excepción de usuarios específicos limitados configuración de configuración de la aplicación [13].

***Plataform as a Service* (PaaS):** La capacidad provista al consumidor es desplegarse en la nube infraestructura creadas o adquiridas por el consumidor creadas mediante lenguajes de programación, bibliotecas, servicios y herramientas compatibles con el proveedor [13].

El consumidor no administrar ni controlar la infraestructura subyacente de la nube, incluida la red, los servidores, sistemas operativos, o almacenamiento, pero tiene control sobre las aplicaciones desplegadas y posiblemente configuración de configuración para el entorno de alojamiento de la aplicación.

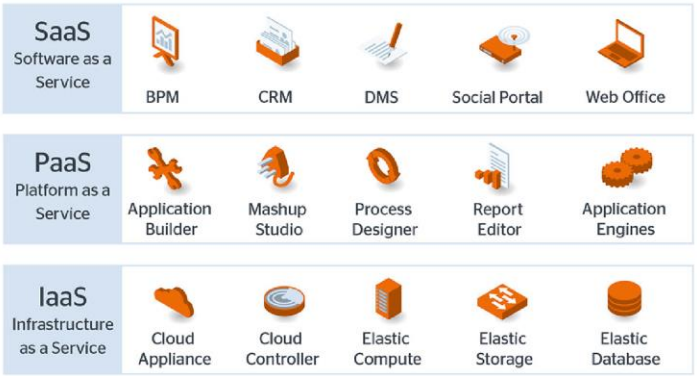


Figura 6 - Modelos de servicio en la nube [15].

2.6 PRINCIPALES PROVEEDORES DE SERVICIOS EN LA NUBE

2.6.1 Microsoft Azure

Microsoft Azure (anteriormente Windows Azure y Azure Services Platform) es un servicio en la nube ofrecida como servicio y alojado en los Data Centers de Microsoft. Anunciada en el Professional Developers Conference de Microsoft (PDC) del 2008 en su versión beta, pasó a ser un producto comercial el 1 de enero de 2010. Windows Azure es una plataforma general que tiene diferentes servicios para aplicaciones, desde servicios que alojan aplicaciones en alguno de los centros de procesamiento de datos de Microsoft para que se ejecute sobre su infraestructura (Nube computacional) hasta servicios de comunicación segura y federación entre aplicaciones. En el reporte de cuadrante mágico de Gartner más reciente, Azure fue uno de solo dos vendedores por las inversiones en código abierto e híbridas en la nube que atraen a las empresas otorgado el título de "Líderes." [8] ver Figura 7.

Figura 7 - Cuadrante mágico para infraestructura como servicio en la nube, en todo el mundo[27]

2.6.1.1 Data centers Microsoft

Figura 8 - Data centers Microsoft a nivel mundial [19]

Microsoft Azure cuenta con 54 data centers y está disponible en 140 países a nivel mundial como se puede ver en figura 8, algunos de ellos ya son centros de datos establecidos **(Availability zones(s) present)**, otras zonas disponibles en la misma región

(Available region) y otras las futuras regiones donde serán instalados los data center **(Announced region).**

Cabe mencionar que, al momento de solicitar algún servicio en la nube, la empresa puede seleccionar la región donde desee el servicio para mayor comodidad, en algunos casos Microsoft recomienda localizaciones adecuadas según el país que solicite el servicio.

2.6.2 Google Platform

Google Cloud Platform (2008). El factor de diferenciación de Google radica en las enormes inversiones que hace en analítica. Muchos clientes que eligen Google tienen aplicaciones ancladas por BigQuery. Según Gartner, "Google suele ser rígido en las negociaciones contractuales, salvo para sus clientes más grandes" [28]. Siempre ha estado presente desde los inicios de la navegación en internet; Google nos ofrece servicios de correo electrónico, respaldo de documentos con Google Drive, Google Calendar, Google Keep (notas rápidas en la nube), etc [26]. Igualmente ofrecen servicios como lo hace Microsoft y VMware

Google Cloud Platform compite con aquellos proveedores de servicios en la nube que ofrecen infraestructura, software o plataformas como servicio; a diferencia de otros Google fue de los primeros en ofrecer servicios en la nube para los desarrolladores, para ello existe Google

App Engine ofrece la creación de distintos lenguajes de desarrollo el cual pueden ser probados e implementados en el mismo momento.

2.6.2.1 Data centers Google

Figura 9 – Data centers Google a nivel Mundial [20]

Como se puede observar en la imagen anterior Google nos ofrece data centers ya establecidos y las futuras regiones donde está instalando sus data centers a nivel mundial;

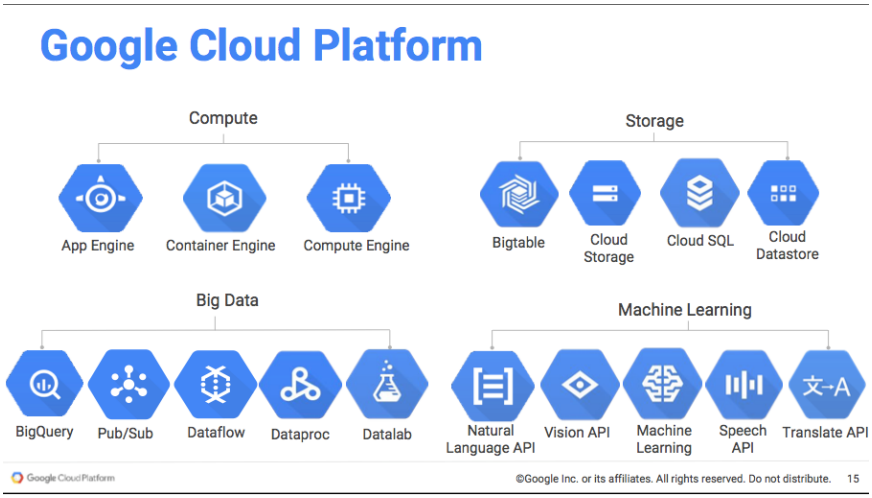


Figura 10 - Servicios de Google Cloud Platform [18]

2.6.2.2 Google Visionario – Cuadrante Mágico de Gartner

Google Cloud Platform está surgiendo como un desafío clave y ocupa el tercer lugar, presentándose como una buena opción para las empresas nativas de la nube. Destaca la portabilidad y su motor de innovación crítica. A pesar de haber iniciado una agresiva guerra de precios contra Amazon, es elegido un proveedor secundario y una alternativa a AWS,

Cabe destacar el ascenso meteórico de Alibaba Cloud, debido principalmente a su posición dominante en China. Su oferta actual muestra un gran potencial de futuro, pero Gartner señala que fuera de China Alibaba Cloud tiene un historial limitado [27].

2.6.3 Listado de Proveedores de IaaS cuadrante mágico de gartner 2017

Los Proveedores analizados en el cuadrante del 2017 son:

- Alibaba Cloud
- Amazon Web Services
- CenturyLink
- Fujitsu
- Google
- IBM
- Interoute
- Joyent
- Microsoft
- NTT Communications
- Oracle
- Rackspace
- Skytap
- Virtustream

2.7 RECUPERACIÓN ANTE DESASTRES COMO SERVICIO (DRaaS)

2.7.1 Definición de Recuperación ante Desastres (DR)

Recuperación ante desastres se comprende como una organización invierte en tecnología (hardware y software) que será usado en casos de desastres que el sitio principal no esté disponible.

2.7.2 Definición de DRaaS

Desde principios de 2000, muchos proveedores de servicios construyeron industrias enteras que reducen el costo y la complejidad de muchas clases de tecnologías. Por ejemplo, Software como servicio (SaaS), Infraestructura como servicio (IaaS), y Plataforma como un servicio (PaaS) han creado completamente nuevos propósitos para el uso de la tecnología por parte de las empresas.

La recuperación de desastres como un servicio (DRaaS) es un rápido crecimiento servicio basado en la nube que facilita a las organizaciones establecer sitios alternativos de procesamiento para recuperación de desastres.

Al igual que otras ofertas "como servicio", el software avanzado permite DRaaS para simplificar todo el proceso para las organizaciones de cualquier tamaño, así como los proveedores de servicios que ofrecen este servicio.

Es importante porque representa una forma innovadora y menos costosa de respaldar datos y sistemas críticos recuperando rápidamente después de un desastre.

Se aprovechan los recursos basados en la nube que proporcionan una infraestructura que está en una zona geográfica distinta, teniendo la capacidad de escalar y compartir recursos de la nube.

2.7.3 Modelos de DRaaS

Public and Prívate Cloud: como lo vimos en los modelos de los servicios en la nube[13], con la única diferencia que las organizaciones están contratando un proveedor de servicios para que les provee la infraestructura, software o la plataforma que desean recuperar en caso de desastres.

Figura 11 - Modelo de recuperación ante Desastres en la Nube [23]

2.7.3.1 Funcionamiento de DRaaS

En general, esta solución se basa en el uso de servidores virtuales en la nube que se utilizan en caso de desastre. Por lo tanto, los usuarios están trabajando en modo nube para respaldo de los datos (es decir, replicados e instalados en estos servidores virtuales en la última operación de copia de seguridad automática). Cuando el problema que causó el incidente está técnicamente resuelto, los datos se pueden reubicar en los servidores locales de la compañía y los usuarios pueden conectarse como de costumbre.

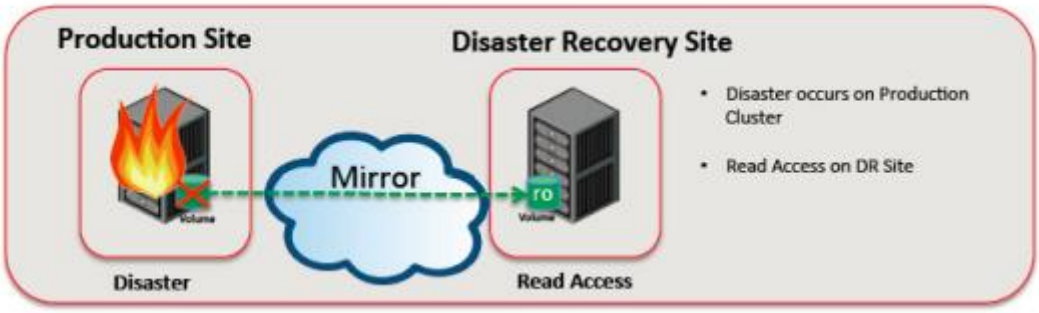


Figura 12 - Funcionamiento General de DRaaS [24]

2.7.4 Cuadrante Mágico de Gartner DRaaS

Figura 13 - Cuadrante Mágico de Gartner junio 2017 [27]

No es recomendable dejarse llevar por la posición del proveedor de servicio DRaaS solo por su posición en el cuadrante de Gartner. Usualmente se tiene como mejor opción las empresas que están en el cuadrante "Líder" pero hay situaciones en las que no es necesario para los objetivos de la empresa, tener todos los servicios que son ofrecidos por las empresas en el cuadrante de Lideres.

Es importante tener en consideración como las empresas van mejorando año con año según el reporte de Gartner, ya que esto nos puede llevar a una alineación entre la empresa y el proveedor de servicio que se elige para brindar el DRaaS.

El reporte de Gartner también brinda una sección llamada Critical Capabilities Report (Reporte de Capacidades Criticas). Este reporte provee una visión profunda del proveedor y sus servicios. Esto ayuda al momento de la toma de decisiones para seleccionar el proveedor adecuado para la empresa, y esta se divide en los siguientes 4 criterios:

- Baja complejidad del ambiente del cliente
- Medio complejidad del ambiente del cliente
- Complejidad del ambiente de clientes para pequeñas empresas
- Complejidad del ambiente de clientes para medianas empresas

III. PLAN DE IMPLEMENTACIÓN DE RECUPERACION ANTE DESASTRES

Para la implementación de un DRP en la nube primero es necesario seguir las siguientes etapas ver Figura 16. Que son conceptos básicos de estrategia de recuperación, recursos y procedimientos requeridos durante la recuperación de los servicios de tecnología de la información y comunicaciones después de una interrupción que permita la continuidad de funciones críticas después de una interrupción.

Cada uno los roles se van ordenan por secuencias como se muestra en la siguiente imagen:

Figura 14 - Secuencia de llamados para la activación de procesos durante el DRP

3.1 Plan de pruebas

Preparar un plan de prueba con diferentes escenarios de interrupción que se utilizará para poner a prueba la integridad y la efectividad del Plan de recuperación de desastres.

Plataforma	Fecha
Servicio/aplicación A	Fecha 1
Servicio/aplicación B	Fecha 2
Servicio/aplicación C	Fecha 3

Tabla 10 - Inventario de Sistemas Críticos

3.2 Revisión del Plan y actualización

Los resultados de las pruebas realizadas en el DRP ofrecen una comprensión del DRP propio y la capacidad del personal para manejar situaciones de interrupción en diferentes escenarios, entendiendo que permitirá a la Empresa alcanzar mejoras (mantenimiento y optimización) y actualizaciones según sea necesario.

3.3 Entrenamiento

El entrenamiento es una actividad que debe llevarse a cabo al menos una vez por año calendario principalmente para aquellos involucrados en el proceso de recuperación ya que esto aporta información para la adecuación del DRP e identifica los recursos necesarios. El entrenamiento facilita la asimilación de los procedimientos en caso de interrupciones en los servicios TI o del negocio.

3.4 Objetivos

Deben de definirse los objetivos y el alcance del plan, de tal manera que, al hacer la implementación del plan, no existan dudas de los resultados. Y evitar trabajos innecesarios en los equipos de trabajo.

3.5 Presunción

Son todas las condiciones reales de la empresa y de los proveedores que influyen directamente en el desarrollo del plan.

3.6 Organización y Responsabilidades del DRP

Para que el proceso de recuperación se desarrolle apropiadamente, la organización del DRP, incluyendo roles y responsabilidades debe ser formalizada, con la siguiente estructura organizacional:

3.6.1 Líder de TI

Es el responsable de la administración del DRP es el líder de tecnología de la Empresa.

Durante un desastre / interrupción, debe:

- Liderar el departamento a través de respuesta a desastres, recuperación del negocio y actividades de reanudación.
- Comunicar la situación y o problemas periódicamente al equipo de gestión de Crisis.

Antes y después de un desastre / interrupción, debe:

- Asegurar una formación adecuada y las pruebas del plan al menos una vez por año calendario.

- Asegúrese de DRP es mantenido y actualizado periódicamente con los cambios en el entorno técnico, personal y proveedores.

3.6.2 Líder de recuperación de negocio

Las tareas del líder de recuperación son las siguientes:

Antes de un desastre / interrupción, debe:
Asegurar la disponibilidad de recursos para la recuperación (documentación, copias, etc.).
Garantizar las condiciones de disponibilidad del sitio de recuperación de continuidad de negocios.

Durante un desastre / interrupción, debe:
• Durante un desastre tiene autoridad para tomar decisiones
• Establecer dirección, estrategias y pasos a seguir para el personal
• Comunicar las actualizaciones, estatus o problemas periódicamente al líder de TI.
• Liderar el departamento a través de respuesta a desastres, recuperación del negocio y actividades de reanudación
• Ser responsable del mantenimiento periódico y actualizaciones del DRP.

Después de un desastre / interrupción, debe:
Elaborar un reporte con la información de la recuperación y rendimiento
Participar en la identificación e implementación de mejoras para el DRP
Documentar y llevar a cabo sesiones de las lecciones aprendidas con los ejecutivos.

3.6.3 Coordinador de recuperación

Antes de un desastre / interrupción, debe:

• Participar en el análisis de impacto en el negocio

• Contribuir en el análisis y diseño de los procedimientos de recuperación

• Tener a mano una copia actualizada de los procedimientos de recuperación y DRP disponibles
• Asegurar que se entrene a los equipos de recuperación

Durante un desastre / interrupción, debe:

• Administrar y proporcionar directrices a los equipos de recuperación
• Comunicar las actualizaciones, estatus o problemas periódicamente con el líder de la recuperación
• Servir de enlace entre los equipos de recuperación y el líder de recuperación.
• Coordinar con otros coordinadores de recuperación
• Comunicarse con proveedores / terceros
• Seguimiento de personal – (anexo A5-Control de colocación de personal).

Después de un desastre, debe:
• Dirigir los equipos de recuperación para restablecer las operaciones al sitio principal
• Colaborar en la labor de restablecer el sitio principal
• Participar en la identificación e implementación de mejoras para el DRP
• Participar en el desarrollo de las lecciones aprendidas

3.6.4 Equipos de recuperación

Los miembros del equipo son responsables de trabajo definido en los procedimientos de recuperación. Estos son sus responsabilidades:

Antes de un desastre / interrupción, deben:
•Apoyar el desarrollo de procedimientos de recuperación y mantenimiento continuo
Participar en la formación

Durante un desastre / interrupción, deben:
• Realizar trabajos de recuperación según el Plan de recuperación y los procedimientos de recuperación
• Documentar y reportar cualquier desviación de los procedimientos documentados

Después de una situación de desastre deben:
• Soporte para regresar a la Página principal
• Colaborar en la actualización del plan de DRP y procedimientos para implementar mejoras
• Participar en el desarrollo de las lecciones aprendidas.

3.7 Procesos y etapas de recuperación de desastres

3.7.1 Plan de activación

La declaración oficial de un evento de interrupción es hecha por el líder de TI que llama a una reunión con los Coordinadores de recuperación para evaluar la magnitud y el impacto de la interrupción. Los coordinadores de líderes y recuperación de TI de las unidades de negocio colaboran para desarrollar una estrategia y un plan de recuperación basados en las circunstancias particulares del evento. El DRP incluye a los equipos de recuperación que necesitan ser activados para comenzar la etapa de recuperación.

3.7.2 Activación de equipos de recuperación

El Coordinador de Recuperación debe usar la información de contacto que se encuentra en el Informe "Información de Personal y Ubicación" (ver anexo 3, cuadro 1) para contactar con los miembros de sus equipos e informar de la situación.

Además, los coordinadores de Recuperación deberán:

1. Documentación de los miembros contactados por medio del “Control de ubicación de Personal”.

2. Manejar un resumen para explicar la situación actual de los miembros del equipo, considerando:

2.1. Resultados de la evaluación de daño inicial

2.2. Tiempo estimado de interrupción

2.3. Objetivos y estrategias que utilizar

2.4. Cualquier consideración de seguridad especial

2.5. Procedimientos de contacto para todo el personal y soporte de recuperación

2.6. Lugar designado para realizar el trabajo de recuperación

2.7. Establecimiento de canales de comunicación entre su estación de trabajo y la ubicación del otro equipo (si se activa un centro de procesamiento alternativo)

2.8. Recordar al personal que no haga declaraciones "públicas" o "fuera de registro" a cualquier representante de los medios de comunicación, entidades públicas u otras entidades.

3.Establecer un mecanismo para manejar las llamadas externas entrantes, para lo cual deberán:

3.1. Utilizar los datos proporcionados en la declaración oficial (de los autorizados a proporcionar información)

3.2. Desarrollar un registro para documentar todas las llamadas entrantes

3.3. Hay que informar que la llamada será devuelta cuando la información requerida esté disponible

3.4. Consulte las consultas críticas con el líder de recuperación para obtener una resolución

4.Mantener la comunicación con el líder de recuperación:

4.1. El Líder de Recuperación envía una lista de personas contactadas y no contactadas

4.2. Realizar cualquier declaración adicional solicitada por el equipo administrador de incidentes o el líder de recuperación

3.7.3 Etapas de respuesta

La declaración oficial de un evento de interrupción es hecha por el líder de TI que llama a una reunión con los coordinadores de recuperación para evaluar la magnitud y el impacto de la interrupción. Los coordinadores de líderes y recuperación de TI colaboran para desarrollar una estrategia y un plan de recuperación basados en las circunstancias particulares del evento. El plan de recuperación incluye a los equipos de recuperación que necesitan ser activados para comenzar la etapa de recuperación.

- Determinar a través del análisis de impacto la magnitud y duración estimada de la interrupción
- Evaluar y priorizar temas específicos
- Desarrollar un plan de recuperación para abordar estas cuestiones desde una perspectiva a corto y largo plazo, según sea necesario
- Incluir la recuperación de aplicaciones críticas identificadas en el Análisis de Impacto Empresarial.
- Incluir la recuperación de la conectividad del usuario a los sistemas críticos
- Identificar equipos de recuperación y preparar el informe "Información sobre el personal" (Anexo 3, Cuadro 1)
- Comunicar el plan de recuperación a los líderes de la gestión de crisis y de las unidades de negocio
- Identificar los lugares de trabajo para el personal de recuperación.
- Organizar un horario de trabajo y rotación basada en la carga de trabajo, recursos y personal disponible.

3.7.4 Etapas de recuperación

En esta etapa, los Coordinadores de Recuperación activan a los Equipos de Recuperación para implementar el Plan de Recuperación elaborado en la etapa anterior:

- Activar e implementar el DRP
- Activar los equipos de recuperación
- Activar el sitio de recuperación.
- Coordinar con proveedores externos para restaurar servicios.
- Identificar los datos de copia de seguridad que se recuperarán del almacenamiento
- Identificar cambios para conectar a los usuarios al sitio de recuperación
- Ejecutar a través del proceso de recuperación hasta la recuperación efectiva de todos los sistemas críticos
- Comunicar las actualizaciones de estado y los problemas
- Mantener un registro de lo que salió bien y mejorar las áreas

3.7.5 Etapas de reanudación

Una vez que la recuperación de todos los sistemas empresariales críticos esté completa, el coordinador de recuperación se centrará en un plan de reanudación para regresar las operaciones en el sitio principal. Una vez que el sitio principal esté disponible, los equipos de recuperación se activan para reanudar las funciones del IT.

- Activar sitio principal
- Coordinar con proveedores externos para restaurar servicios al sitio principal
- Identificar los datos de copia de seguridad que se recuperarán del almacenamiento
- Activar y aplicar el plan de reanudación
- Comunicar cambios para conectar a los usuarios al sitio principal
- Ejecutar a través del proceso de reanudación hasta la reanudación efectiva de todos los sistemas
- Comunicar las actualizaciones de estado y los problemas
- Eliminar todos los datos del sitio alternativo
- Desactivar sitio alternativo
- Mantener un registro de lo que salió bien y mejorar las áreas

3.7.6 Comunicación

Los canales de comunicación tienen que estar bien gestionados durante un desastre. El líder de IT es responsable de reportar actualizaciones de estado a la administración de crisis y líderes de negocio.

El Coordinador de recuperación es responsable de comunicar y coordinar con otros coordinadores de recuperación, proveedores de servicios de terceros y mantener la información fluyendo entre los equipos de recuperación.

Todas las comunicaciones con los usuarios finales serán coordinadas y conducidas por los equipos de la oficina de servicios generales de las unidades de negocio.

Los controles que son necesarios para documentar el DRP, y que deben de estar disponibles para los equipos.

IV. CONCLUSIONES

Todas las instituciones educativas sin importar su tamaño deben de integrar a sus procesos un Plan de Recuperación ante desastres (DRP), para garantizar la integridad y la disponibilidad de la información que las hace funcionar, cuando se presente algún evento repentino y fortuito que amenace la información.

Existe conocimiento de la necesidad de contar con un plan de recuperación puesto que cinco de las seis instituciones educativas; poseen un sitio para recuperación en caso de desastre.

Cuatro de seis instituciones educativas, han implementado el proceso de recuperación ante desastres, en el cual se han identificado los procesos más críticos para ellas.

En las instituciones educativas encuestadas, se observa que sin tener el otro centro de datos como contingencia utilizan algún servicio en la nube computacional, lo que nos indica que existe la suficiente confianza del uso de esta tecnología.

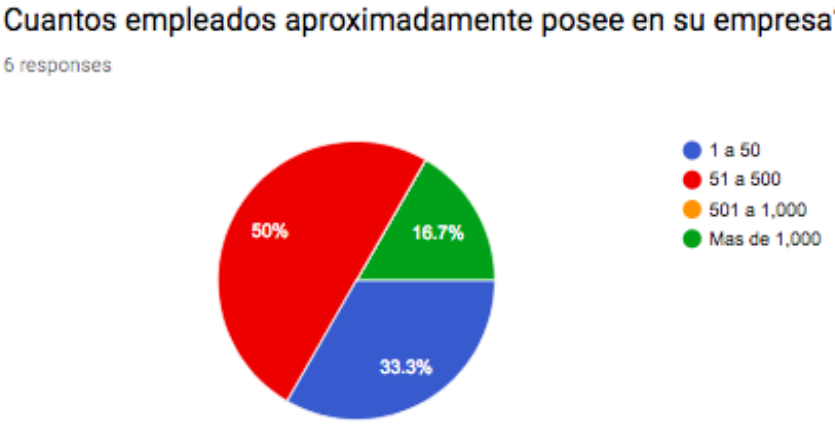
Ninguna institución educativa utiliza el servicio de DRaaS, por lo que, con el marco de referencia, y toda la información concerniente a este servicio indicadas en este documento, pueden ampliar algunos conceptos y ampliar su conocimiento para tomar criterios de los riesgos que tiene no tener un respaldo de su información y evaluar la factibilidad de implementarlo y las estrategias técnicas y económicas para hacerlo posible a corto plazo.

V. LIMITACIONES

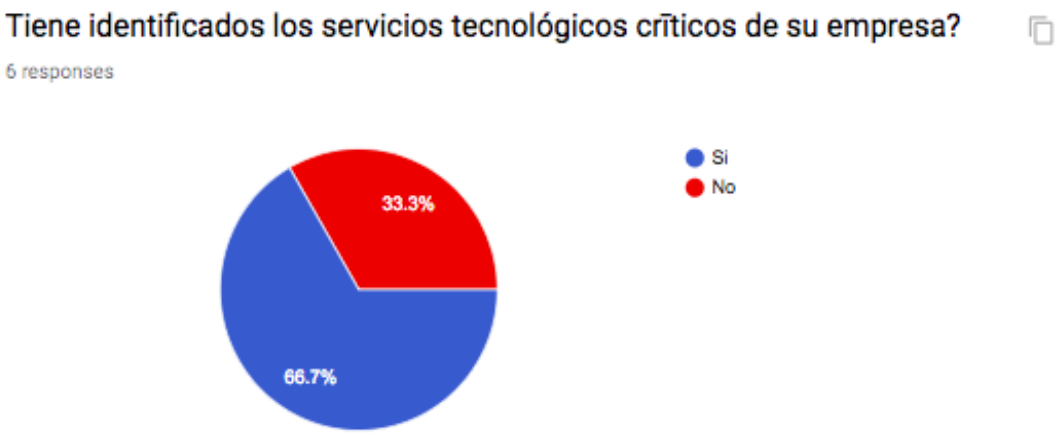
Dentro del análisis realizado para la implementación de un DRP en la nube se consideraron diez instituciones educativas del área metropolitana, cuatro de ellas respondieron con el argumento de no divulgar información de su infraestructura tecnológica y/o sistemas de información y otras simplemente no dieron apertura al estudio a realizar por lo cual solo se tomaron seis instituciones para el presente tema de investigación.

VI. RESULTADOS DE LA ENCUESTA

Grafica 1 - Contingencia de Información

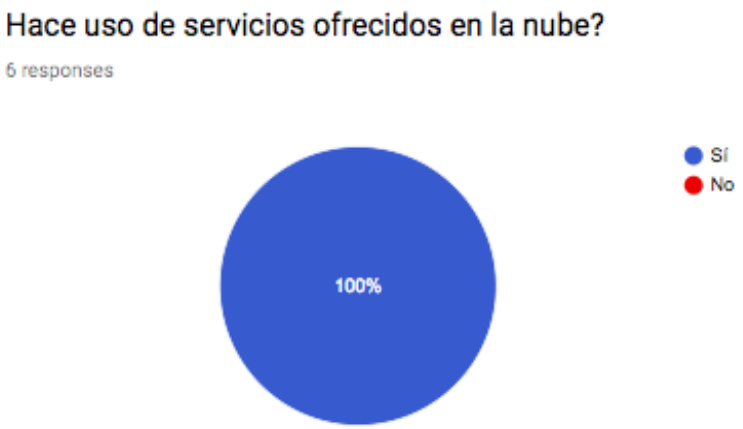


Grafica 2 - Cantidad de Empleados

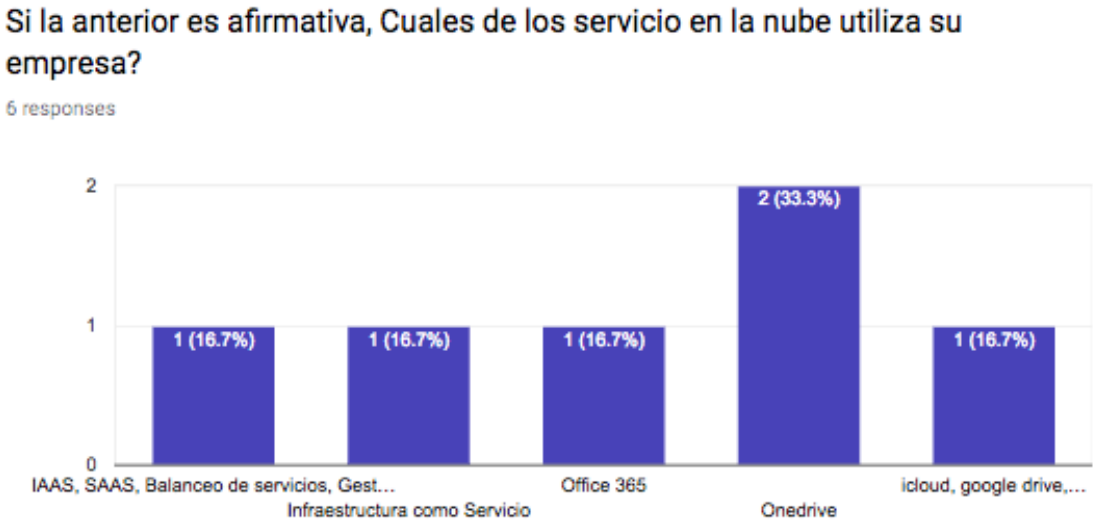


Grafica 3 - Sistemas Críticos

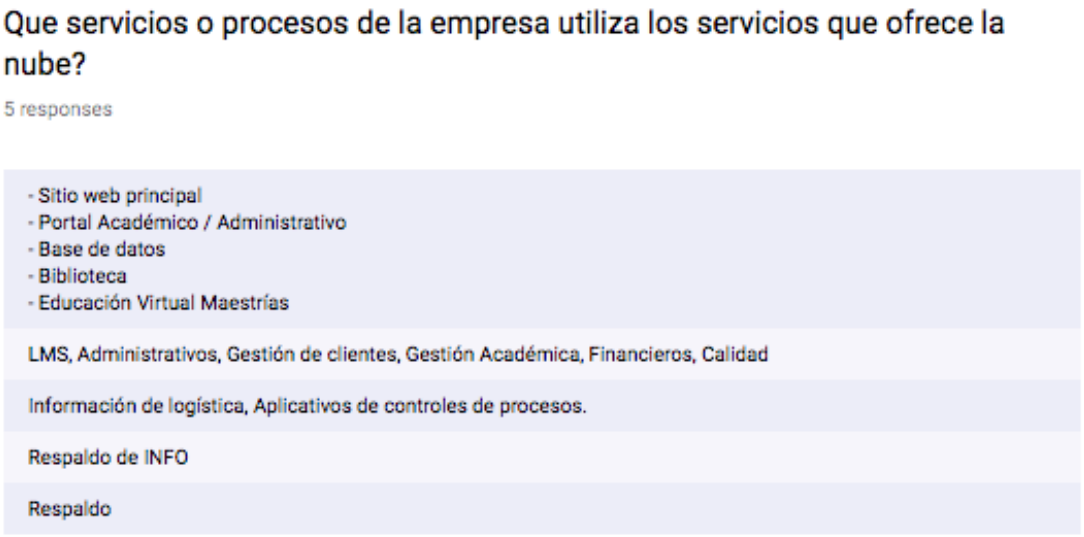
Grafica 4 - Plan ante desastres de los sistemas críticos.



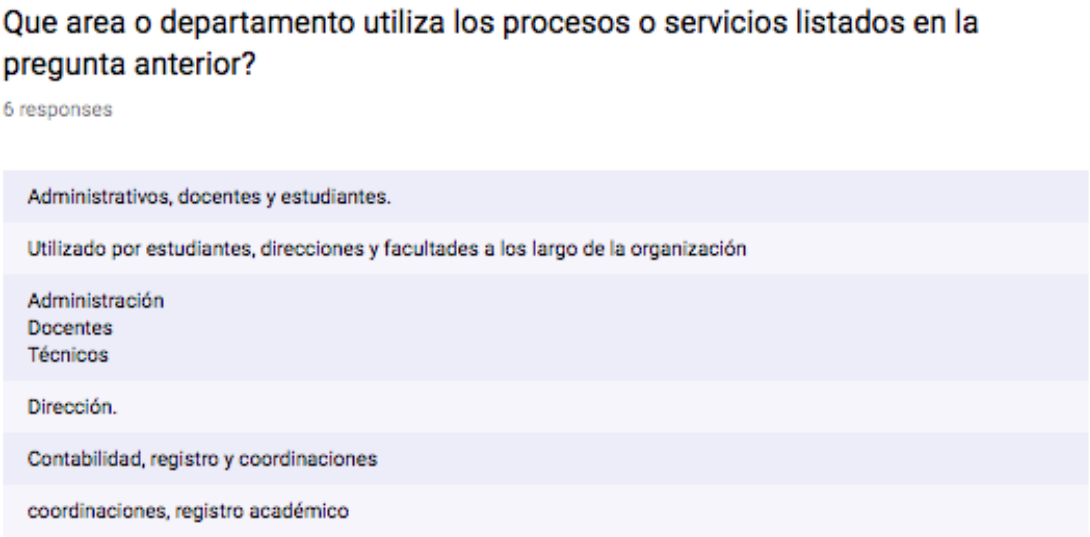
Grafica 5 - Uso de los servicios de la nube.



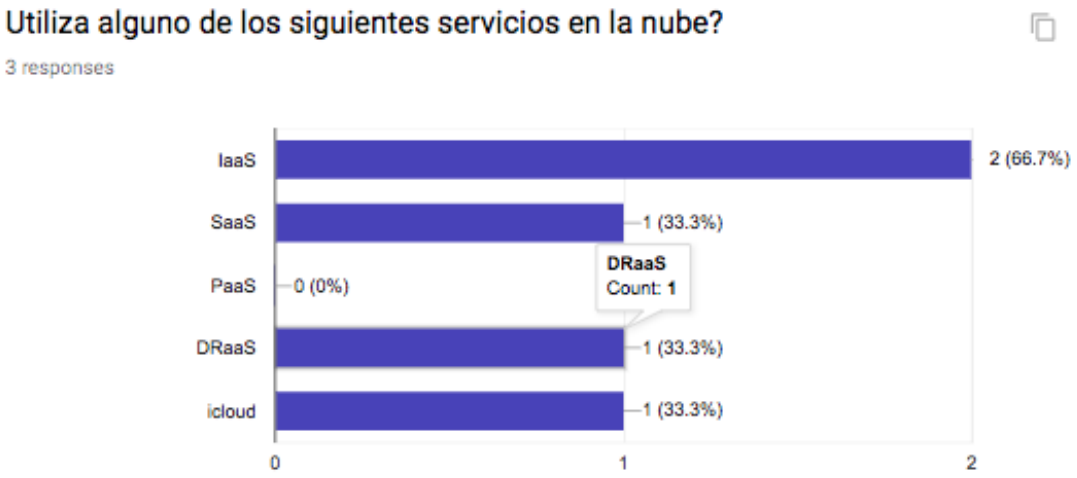
Grafica 6 - Uso de los servicios en la nube



Grafica 7 - Servicios Críticos de las instituciones en la nube



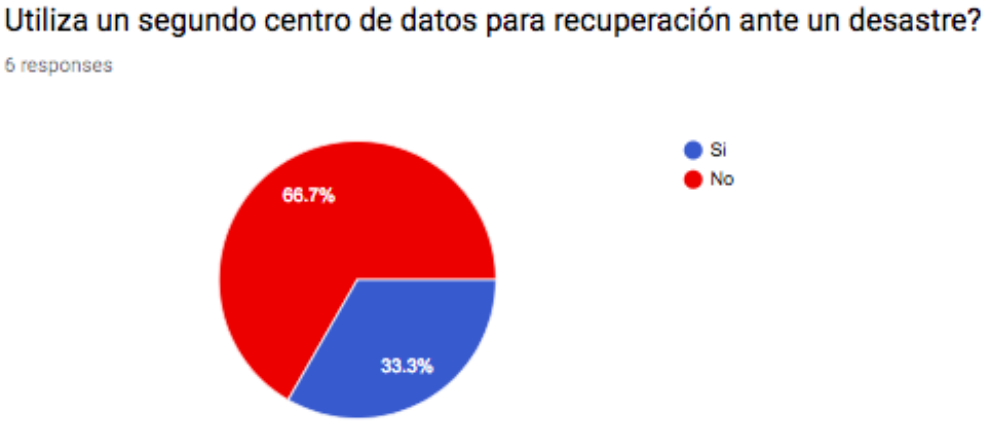
Grafica 8 - Áreas que utiliza los servicios de la nube.



Grafica 9 - Utilización de las plataformas de la nube.

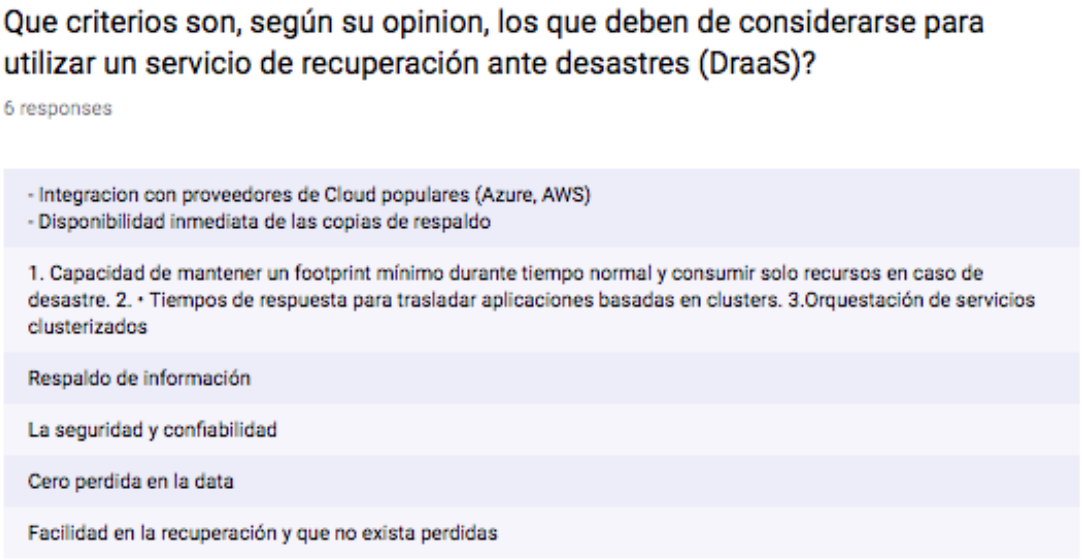
Grafica 10 - Proveedores de servicios en la nube.

Grafica 11 - Uso de los servicios de la nube - DRAaS



Grafica 12 - Centro de datos de contingencia de las instituciones

Grafica 13 - Proveedores de Servicios en El Salvador



Grafica 14 - Consideraciones de las instituciones para usar los Servicios DRAaS

VII. BIBLIOGRAFIA

[1] Europea, C. E. (s.f.). Implementación del programa comunitario Lisboa. Obtenido de una política moderna de la PYME: https://publications.europa.eu/en/publication-detail/-/publication/6eeedf23-4251-4fbb-a866-d7a9d0b82c22/language-es/format-PDF

[2] OIT. (2013). Material de formación sobre evaluación y riesgo. Obtenido de para PYMES: https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---

[3] CONAMYPE, M. d. (2014). Ley de Fomento Protección y Desarrollo para la Micro y pequeña Empresa. San Salvador, El Salvador

[4] Ing. Juan Carlos Angarita C., M. (s.f.). Traducción no oficial – Uso académico. Obtenido de International Organization for Standardization - ISO 22301:2012: https://www.iso.org/standard/50038.html

[5] Consultorias, G. A. (30 de Octubre de 2017). Beneficios de implementar un DRP (Disaster Recovery Plan) en las Organizaciones. Obtenido de http://www.grupoalbe.com/beneficios-de-implementar-un-drp-disaster-recovery-plan-en-las-organizaciones-pymes/

[6] Template, D. R. (2013). Difference Between DRP and BCP. Obtenido de http://www.disasterrecoveryplantemplate.org/difference-between-drp-and-bcp/

[7] Mell, P., & Timothy , G. (s.f.). NIST Cloud Computing Resources. Obtenido de Effectively and Securely Using the Cloud Computing Paradigm: http://csrc.nist.gov/groups/SNS/cloud-computing/index.html

[8] Wikipedia. (s.f.). La enciclopedia libre. Obtenido de https://es.wikipedia.org/wiki/Microsoft_Azure

[9] Gregory, P. (2016). DraaS for Dummies. Obtenido de http://cstor.com: http://cstor.com/wp-content/uploads/2017/06/Veeam_DRaaS_for_Dummies_eBook.pdf

[10] Alhazmi, O. H., & Malaiya, Y. (2013). Evaluating Disaster Recovery Plans Using the Cloud. *IEEE Papers*.

[11] BSIgroup. (s.f.). *ISO 22301 para pequeñas y medianas empresas (PYMES)*. Obtenido de https://www.bsigroup.com/es-PE/gestion-de-la-continuidad-del-negocio-iso-22301-/iso-22301-para-pymes/

[12] SIAYEC, G. (s.f.). *Beneficios de implementar un DRP (Disaster Recovery Plan) en las Organizaciones*. Obtenido de https://www.bsigroup.com/es-PE/gestion-de-la-continuidad-del-negocio-iso-22301-/iso-22301-para-pymes

[13] Mell, P., & Timothy , G. (2011). The NIST Definition of Cloud Computing

[14] ESET. (s.f.). *¿En qué consiste un Plan de Recuperación ante Desastres (DRP)?* Obtenido de https://www.welivesecurity.com/la-es/2014/10/14/plan-de-recuperacion-ante-desastres/

[15] Software, D. (s.f.). *Cloud Computing* . Obtenido de http://www.digitalsoftwareinc.com/cloud_computing.html

[16] INFORMÁTICA, N. (s.f.). *Tipos de nubes*. Obtenido de http://nubeinformaticaexpo.blogspot.com/p/tipos-de-nubes.html

[17] Google, S. (s.f.). *Trabajo Final LA NUBE*. Obtenido de https://sites.google.com/site/exceedengllishlife/la-nube

[18] Gallego, J. L. (s.f.). *Dar permisos públicos de lectura a un bucket en Google Cloud Storage*. Obtenido de https://joseluisgv.com/dar-permisos-publicos-de-lectura-a-un-bucket-en-google-cloud-storage/

[19] MIcrosoft. (s.f.). *Azure regions*. Obtenido de https://azure.microsoft.com/en-us/global-infrastructure/regions/

[20] Cloud, G. (s.f.). *Ubicaciones de Cloud*. Obtenido de https://cloud.google.com/about/locations/

[21] Symantec. (s.f.). *Disaster Recovery Study*. Obtenido de Global Results: http://www.symantec.com/content/en/us/about/media/pdfs/Symc_Survey_SAMGDisasterRecovery_Global_2010.pdf

[23] HPT, C. (s.f.). *Business case for DRaaS Solution*. Obtenido de https://cdn2.hubspot.net/hubfs/169136/docs/The_Business_Case_for_Disaster_Recovery_as_a_service_v2.pdf?t=1485165472106

[24] MAPR. (s.f.). *Disaster Recovery*. Obtenido de https://mapr.com/resources/disaster-recovery/

[25] Greenhouse, S. (s.f.). *RPO y RTO*. Obtenido de https://www.swgreenhouse.com/conceptos-de-continuidad-de-negocio/rto-rpo

[26] Wikipedia. (s.f.). *Google Cloud Platform*. Obtenido de https://en.wikipedia.org/wiki/Google_Cloud_Platform

[27] TECNOZERO. (s.f.). *Cuadrante de Gartner IaaS 2018*. Obtenido de https://www.tecnozero.com/blog/cuadrante-de-gartner-iaas-2018/

[28] https://www.tecnozero.com/blog/cuadrante-de-gartner-iaas-2018/

Inc., G. (s.f.). About the GCP services. Obtenido de https://cloud.google.com/docs/overview/cloud-platform-services

Inc., G. (s.f.). Google cloud. Obtenido de https://cloud.google.com/docs/overview/

Inc., G. (s.f.). Google cloud. Obtenido de How to Design a Disaster Recovery Plan : https://cloud.google.com/solutions/designing-a-disaster-recovery-plan

Inc., G. (s.f.). Google Cloud. Obtenido de Compute Engine: https://cloud.google.com/compute/

Inc., M. (s.f.). Infraestructura como un servicio. Obtenido de https://azure.microsoft.com/es-es/overview/what-is-iaas/

Inc., M. (s.f.). Microsoft. Obtenido de What is IaaS: https://azure.microsoft.com/es-es/overview/what-is-iaas/.

Inc., M. (s.f.). Microsoft AZURE. Obtenido de https://azure.microsoft.com/es-es/overview/what-is-cloud-computing/

Inc., M. (s.f.). Microsoft site recovery. Obtenido de https://azure.microsoft.com/es-es/services/site-recovery/

Inc., M. (s.f.). Plataforma como un servicio. Obtenido de https://azure.microsoft.com/es-es/overview/what-is-paas/

Inc., M. (s.f.). Software como un servicio. Obtenido de https://azure.microsoft.com/es-es/overview/what-is-saas/

Ing. Juan Carlos Angarita C., M. (s.f.). Traducción no oficial – Uso académico. Obtenido de International Organization for Standardization - ISO 22301:2012: https://www.iso.org/standard/50038.html

Symantec. (2010). Symantec 2010 Disaster Recovery Study. Obtenido de Global: http://www.symantec.com/content/en/us/about/media/pdfs/Symc_Survey_SAMGDisasterRecovery_Global_2010.pdf

Wikipedia. (s.f.). Google Compute Engine - History. Obtenido de https://en.wikipedia.org/wiki/Google_Compute_Engine

H. B. S. Hassen BEN REBAH, «Disaster Recovery as a Service, A Disaster Recovery Plan in the Cloud for SMEs,» Global Summit on Computer & Information Technology, 2016.

VIII. GLOSARIO

Almacenamiento: es un concepto que se utiliza para hacer referencia a un acto mediante el cual se guarda algún objeto o elemento específico con el fin de poder luego recurrir a él en el caso que sea necesario

BCP (Business Continuity Plan): es un plan logístico para la práctica de cómo una organización debe recuperar y restaurar sus funciones críticas parcialmente o totalmente interrumpidas dentro de un tiempo predeterminado después de una interrupción no deseada o desastre.

CONAMYPE: Comisión nacional de la micro y pequeña empresa de El Salvador.

Confidencialidad: es la propiedad de la información, por la que se garantiza que no está accesible únicamente a personal autorizado a acceder a dicha información.

Disponibilidad: algo que está libre para usarse y de lo que se puede disponer libremente.

DRP: Plan de recuperación ante desastres es un proceso de recuperación que cubre los datos, el hardware y el software crítico, para que un negocio pueda comenzar de nuevo sus operaciones en caso de un desastre natural o causado por humanos.

DRaaS: Recuperación ante Desastres como servicio es un modelo de servicio de copia de seguridad y computación en la nube que utiliza los recursos de la nube para proteger las aplicaciones y los datos de las interrupciones causadas por un desastre.

Elasticidad: es una medida de la sensibilidad de la cantidad demandada de un bien ante un cambio en su precio. La elasticidad busca medir el impacto, o el grado de las variaciones de las demandas o las ofertas de los productos dadas diversas variaciones de precios.

Failover: La conmutación por error, o failover, es un modo de funcionamiento de respaldo en el que las funciones de un componente de sistema (tal como un procesador, servidor, red o base de datos, por ejemplo) son asumidos por componentes del sistema secundario cuando el componente principal no está disponible ya sea debido a una falla o por el tiempo de inactividad programado.

IaaS (Infraestructura como servicio) : es una infraestructura informática inmediata que se aprovisiona y administra a través de Internet. Permite reducir o escalar verticalmente los recursos con rapidez para ajustarlos a la demanda y se paga por uso.

Infraestructura Tecnológica: Se podría definir como el conjunto de elementos para el almacenamiento de los datos de una empresa. En ella se incluye el hardware, el software y los diferentes servicios necesarios para optimizar la gestión interna y seguridad de información.

Integridad: es la capacidad que tiene de actuar en consecuencia con lo que se dice o lo que se considera que es importante ya sea algo íntegro que se trata de un elemento que tiene todas sus partes enteras.
ITIL: es un marco de trabajo de buenas prácticas aplicables a la Gestión de Servicios de TI y definidas para ayudar a las organizaciones proveedoras de servicios de TI a conseguir una mayor calidad y eficiencia en la entrega y gestión de sus servicios.

PYMES: Un término relacionado es mi pyme o MIPyME, el acrónimo de micro, pequeña y mediana empresa, que toma en cuenta las modalidades de empresa más reducidas, tales como las unipersonales.

NIST: Instituto Nacional de Estándares y Tecnologías es una agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos. La misión de este instituto es promover la innovación y la competencia industrial en Estados Unidos mediante avances en metrología, normas y tecnología de forma que mejoren la estabilidad económica y la calidad de vida.

Normas ISO: La palabra ISO deriva de la palabra griega “isos”, que significa “igual”. La definición larga es que las siglas hacen referencia a “Organización Internacional de Normalización”

Nube Computacional: conocida también como servicios en la nube, informática en la nube, nube de cómputo, nube de conceptos o simplemente "la nube", es un paradigma que permite ofrecer servicios de computación a través de una red, que usualmente es Internet.

Replicación asíncrona: Una vez que los datos han sido escritos en el sitio de almacenamiento primario, nuevas escrituras a ese sitio pueden ser aceptadas, sin tener que esperar que el sitio de almacenamiento secundario o remoto también termine su escritura.

Replicación síncrona: El modo síncrono implica que las escrituras en la aplicación se mantengan inactivas hasta que los datos lleguen al sitio secundario o remoto. Una vez que las escrituras se efectúan, se reconocen en la aplicación.

Riesgo: posibilidad de que se produzca un contratiempo o una desgracia, de que alguien o algo sufra perjuicio o daño.

RPO (Recovery Point Objective): Determina el objetivo de posible pérdida máxima de datos introducidos desde el último backup, hasta la caída del sistema, y no depende del tiempo de recuperación.

RTO (Recovery Time Objective): Objetivo de Tiempo de Recuperación: Expresa el tiempo durante el cual una organización pueda tolerar la falta de funcionamiento de sus aplicaciones y la caída de nivel de servicio asociada, sin afectar a la continuidad del negocio.

SGCN: Un Sistema de Gestión de Continuidad de Negocio (SGCN) ayuda a las organizaciones a establecer estructuras para identificar posibles amenazas, el impacto de los incidentes y cómo pueden protegerse frente a estas.

PaaS: Plataforma como servicio (PaaS) es un entorno de desarrollo e implementación completo en la nube, con recursos que permiten entregar todo, desde aplicaciones sencillas basadas en la nube hasta aplicaciones empresariales sofisticadas habilitadas para la nube.

PHVA: El ciclo PHVA de mejora continua es una herramienta de gestión presentada en los años 50 por el estadístico estadounidense Edward Deming.

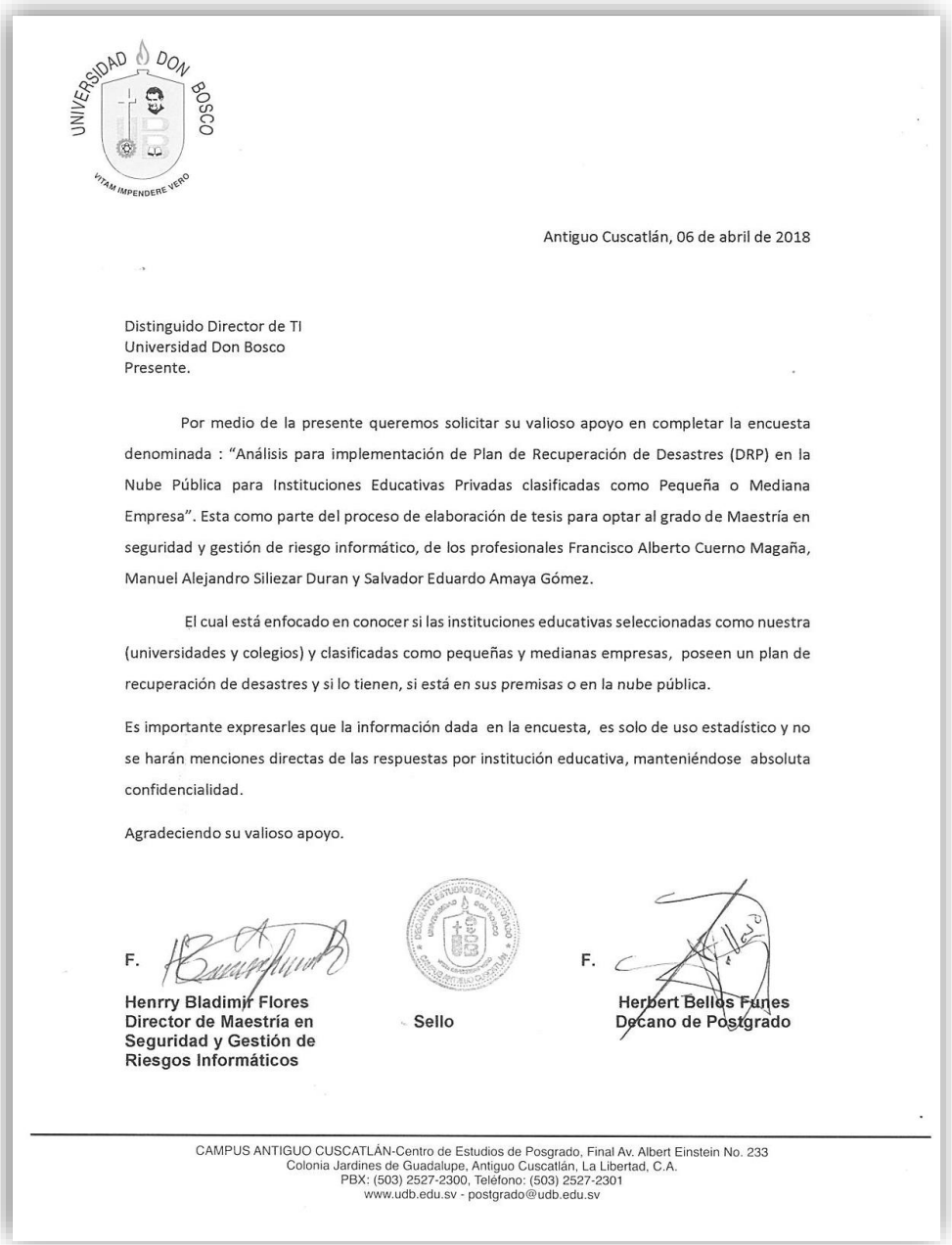
Recuperación: es la acción y efecto de recuperar o recuperarse (volver en sí o a un estado de normalidad, volver a tomar lo que antes se tenía, compensar).

SaaS: Software como servicio permite a los usuarios conectarse a aplicaciones basadas en la nube a través de Internet y usarlas. Algunos ejemplos comunes son el correo electrónico, los calendarios y las herramientas ofimáticas (como Microsoft Office 365).

Virtualización: es la creación a través de software de una versión virtual de algún recurso tecnológico, como puede ser una plataforma de hardware, un sistema operativo, un dispositivo de almacenamiento u otros recursos de red

IX. ANEXOS

ANEXO 1. Modelo de carta entrega a las instituciones educativas del sector privado autorizada por la Universidad Don Bosco del área de Postgrados



Antiguo Cuscatlán, 06 de abril de 2018

Distinguido Director de TI
Universidad Don Bosco
Presente.

Por medio de la presente queremos solicitar su valioso apoyo en completar la encuesta denominada : "Análisis para implementación de Plan de Recuperación de Desastres (DRP) en la Nube Pública para Instituciones Educativas Privadas clasificadas como Pequeña o Mediana Empresa". Esta como parte del proceso de elaboración de tesis para optar al grado de Maestría en seguridad y gestión de riesgo informático, de los profesionales Francisco Alberto Cuerno Magaña, Manuel Alejandro Siliezar Duran y Salvador Eduardo Amaya Gómez.

El cual está enfocado en conocer si las instituciones educativas seleccionadas como nuestra (universidades y colegios) y clasificadas como pequeñas y medianas empresas, poseen un plan de recuperación de desastres y si lo tienen, si está en sus premisas o en la nube pública.

Es importante expresarles que la información dada en la encuesta, es solo de uso estadístico y no se harán menciones directas de las respuestas por institución educativa, manteniéndose absoluta confidencialidad.

Agradeciendo su valioso apoyo.

F.

Henrry Bladimir Flores
Director de Maestría en Seguridad y Gestión de Riesgos Informáticos

Sello

F.

Herbert Bellos Funes
Decano de Postgrado

CAMPUS ANTIGUO CUSCATLÁN-Centro de Estudios de Posgrado, Final Av. Albert Einstein No. 233
Colonia Jardines de Guadalupe, Antiguo Cuscatlán, La Libertad, C.A.
PBX: (503) 2527-2300, Teléfono: (503) 2527-2301
www.udb.edu.sv - postgrado@udb.edu.sv

ANEXO 2. Controles para etapas del DRP

Información sobre el personal y las ubicaciones

Roles	Nombre	Teléfono Oficina	Teléfono Móvil	Teléfono de Casa	Suplente
Líder de TI					
Líder del sitio de recuperación					
Líder de recuperación					
Coordinador de sitio de recuperación					
Coordinador de recuperación					

Información sobre las ubicaciones

Lugar	Responsable	Dirección	Teléfono 1	Teléfono 2
Centro de Procesamiento Principal				
Sitio de recuperación de continuidad empresarial				

Sitio de recuperación de continuidad empresarial

Nombre de Cliente		
Número de Cliente		
Dirección		
Teléfono		
Horario		
Vencimiento de Contrato		
Contacto		
Nombre:		
Teléfono de Oficina		
Teléfono Celular		
Email		

Sitio para la protección de datos (copia de seguridad)

Dirección de la compañía	
Teléfono	
Horario	
Tipo de Datos	

Contactos de terceros / proveedores

Compañía				
Servicio Soportado				
Servicio Existente				
Nivel de Servicio				
Teléfono de Compañía				
Fax de Compañía				
Dirección				
E-Mail				
Contactos	**E-mail**	**Teléfono**	**Celular**	**Ubicación**

Control de ubicación del personal

Objetivo	Mantener un control centralizado de la ubicación del personal
Procedimiento para los líderes de equipo	● Obtenga copias de este formulario ● Completar después de la activación del Plan para el control correspondiente ● Realizar comprobaciones durante el proceso de recuperación
Códigos de Ubicación	1. Empleado no contactado, mensaje dejado 2. Empleado en el lugar de trabajo 3. Empleado fuera del lugar de trabajo 4. El empleado sugirió reportarse al sitio del desastre y ayudar con la recuperación 5. Ubicado en el sitio alternativo 6. El empleado sugirió quedarse en casa hasta nuevo aviso
Fecha	_____

NOMBRE DE CONTACTO	TELÉFONO	CÓDIGO DE UBICACIÓN	FECHA	HORA