FACULTAD DE INGENIERÍA

Carrera de Ingeniería Empresarial y de Sistemas

MIGRACIÓN DE SERVIDORES A LA NUBE DE MICROSOFT AZURE PARA MEJORAR LA CONTINUIDAD DE LOS SERVICIOS TI, DE LA FIDUCIARIA EN EL AÑO 2018

Tesis para optar el Título Profesional de Ingeniero Empresarial y de Sistemas

ANGEL JUNIOR RUIZ CALDAS

Asesor:
Marco Antonio Salcedo Huarcaya

Lima – Perú
2019

ÌNDICE DE CONTENIDOS

ÌNDICE DE FIGURAS

ÍNDICE DE TABLA

Introducción

El presente trabajo de suficiencia profesional fue desarrollado en base a un proyecto que permitió poder realizar la implementación de una adecuado plan de continuidad de los servicios críticos de la empresa, mediante la migración de los servidores físicos a la nube de la empresa La Fiduciaria, con una herramienta y arquitectura de Microsoft Azure, para así poder contar con un adecuado plan de contingencia de los servicios.

La actividad empresarial implica la existencia de diversos niveles de riesgos de operación; los mismos que cada empresa debe detectar, analizar y establecer las medidas preventivas a fin de mitigar su posible impacto.

La gestión de riesgos de operación de una empresa consiste en la función de su tamaño y complejidad de sus operaciones. Es así que los riesgos de una determinada industria no son los mismos que se pueden determinar en la actividad bancaria y financiera. De igual forma dentro de la actividad bancaria es necesario evaluar los procesos que realiza cada empresa del sector a fin de determinar cuáles son los riegos que enfrenta, las medidas de control establecidas, el monitoreo de la evolución de dichos riesgos y los niveles de contingencia que la empresa puede asumir.

Si bien no todos los riegos pueden ser eliminados la empresa se encuentra en la obligación de establecer todos los controles posibles a fin de mitigar el posible impacto de los mismos.

La implementación de este proyecto utiliza los elementos y medios necesarios para una adecuada solución utilizando la tecnológica de Microsoft Azure.

Desarrollo

En la actualidad las compañías, grandes o pequeñas, depositan su activo más preciado en sistemas informáticos: sus datos, su información, sin embargo, son muy pocas las que implementan un adecuado plan de contingencia de los servicios críticos.

No es suficiente contar con un poderoso antivirus o mantener un backup diario de la información pensando que eso mantendrá segura la información, sino es necesario contar con procedimientos y herramientas alternativos que permitan ante alguna contingencia mantener los servicios críticos de la empresa activos. Estos procedimientos alternativos a la operación normal se le llama Plan de Contingencia.

Este tipo de Plan tiene como misión minimizar los perjuicios que sufrirá una empresa cuando una eventualidad altere el trabajo normal del sistema informático. El mismo es desarrollado para proveer la mejor habilidad posible de recuperación en el caso de que las medidas normales de seguridad no fueran efectivas y ha ocurrido alguna pérdida de información.

Capítulo I: Generalidades de la Empresa

Datos Generales

La Fiduciaria es una de las empresas líderes en el sector fiduciario. Fue fundada en el año 2001 y hasta la actualidad se ha establecido como una empresa líder en el mercado fiduciario con un promedio de participación del 50% en el mercado peruano. Esto permite poder ofrecer soluciones novedosas y una administración transparente a sus clientes.

Nombre o Razón Social de la Empresa

LA FIDUCIARIA S.A.
RUC: 20501842771

Ubicación de la Empresa

- Dirección Legal: Cal. los Libertadores Nro. 155 Dpto. 8
- Distrito / Ciudad: San Isidro
- Departamento: Lima, Perú

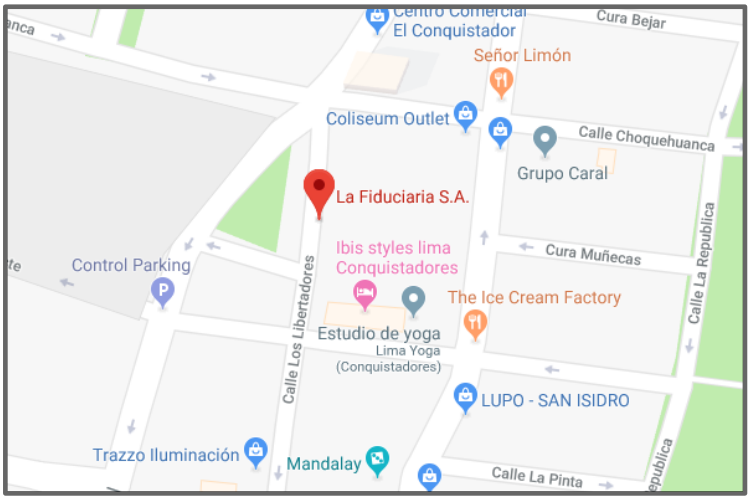


Figura 1. Ubicación de la empresa
Fuente: Recuperado de https://www.google.com/maps

Giro de la empresa

Administración de fideicomisos.

Tamaño de la empresa

La empresa cuenta con un total de 70 trabajadores.

Reseña histórica de la empresa

En el año 2002, las entidades, el grupo crédito, Interbank y el banco Scotiabank fundaron la primera empresa fiduciaria del Perú. Con el objetivo de poder dar a conocer el servicio de fideicomiso en el Perú, brindando transparencia, seguridad y confianza en todas sus operaciones.

Organigrama de la Empresa

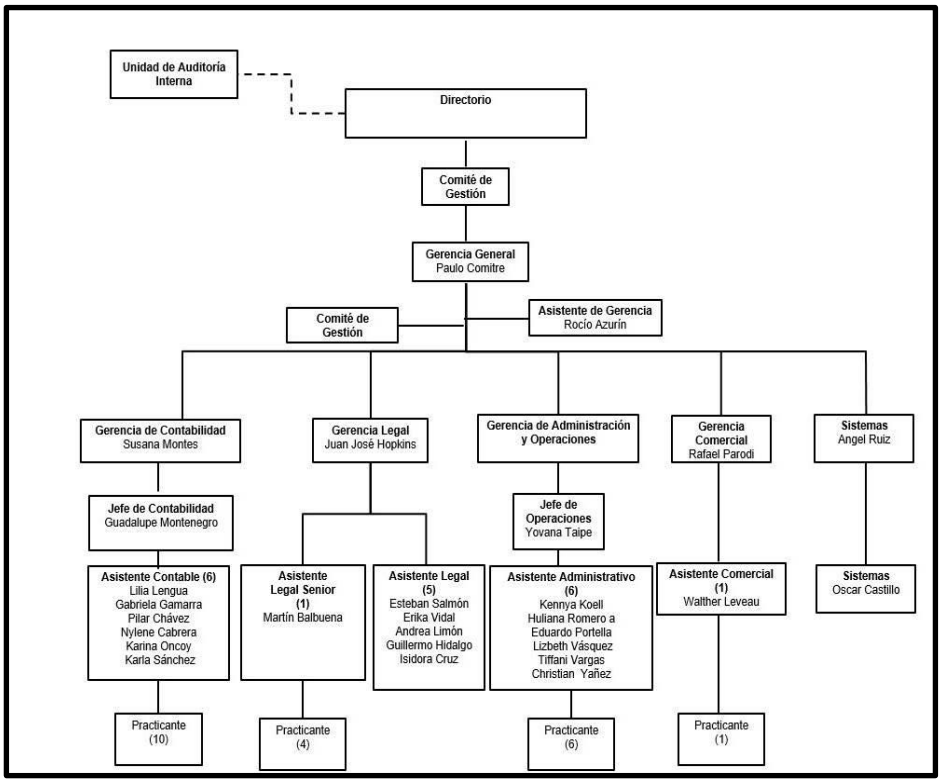


Figura 2. Organigrama de la Empresa
Fuente: Recuperado de https://www.lafiduciaria.com.pe/

Misión, Visión y Política

Misión

Contar con una adecuada cultura organizacional enfocada en la excelencia del servicio, con un personal altamente capacitado que permita el desarrollo de productos innovadores y flexibles que esté basado en la confianza de los clientes comprometidos.

Visión

Convertirse en la empresa líder del sector fiduciario, ofreciendo confianza y compromiso con sus clientes.

Políticas

- Generar confianza para sus clientes administrando sus bienes fideicometidos con transparencia.
- Participar en el crecimiento y desarrollo de las estructuras financieras para el desarrollo del ámbito nacional.
- Desarrollar servicios que se adapten al requerimiento de los clientes.
- Fomentar la cultura organizacional comprometida en la excelencia del servicio.

Servicios y clientes

El fideicomiso es un servicio de administración que involucra a tres partes , el fideicomitente(quien aporta) entrega sus bienes en fideicomiso a otra persona llamada fiduciario (La Fiduciaria), para que se constituya un patrimonio autónomo, sujeto al control fiduciario bajo el cumplimiento de un fin específico a favor del fideicomitente o un fideicomisario(el beneficiario).

La cartera de clientes de la empresa abarca los rubros, financieros, construcción, educación.

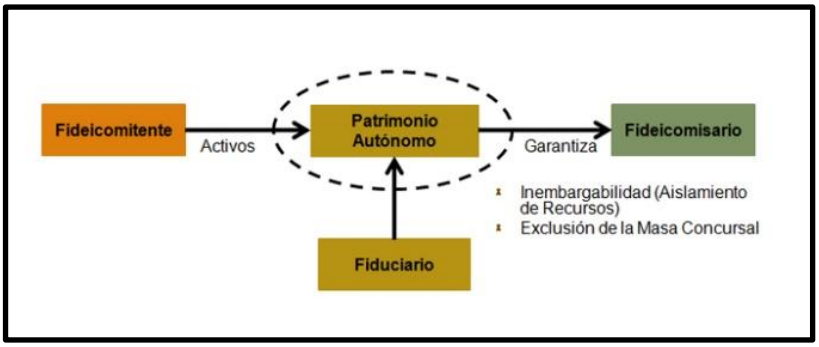


Figura 3. Flujo del Fideicomiso
Fuente: Recuperado de https://www.lafiduciaria.com.pe/

Premios y Certificaciones

Se otorgaron a la empresa reconocimientos de diferentes instituciones del Perú.

Relación de la Empresa con la Sociedad

Cumpliendo con sus principios y siempre comprometidos con el bienestar de la sociedad, mantienen participación activa en programas de ayuda a miembros de la comunidad como:

- Teletón
- cuerpo de bomberos del Perú
- pro mujer
- magia cura el cáncer

Capítulo II: Planteamiento del Problema

¿Cómo contar con un adecuado plan de continuidad ante un desastre, ataque o falla de servicios TI de la empresa la fiduciaria?

Una de las principales causas que afectan la continuidad del negocio son los ataques cibernéticos, el diario Gestión realizó una encuesta a las empresas peruanas en el año 2019 obteniendo lo siguiente:

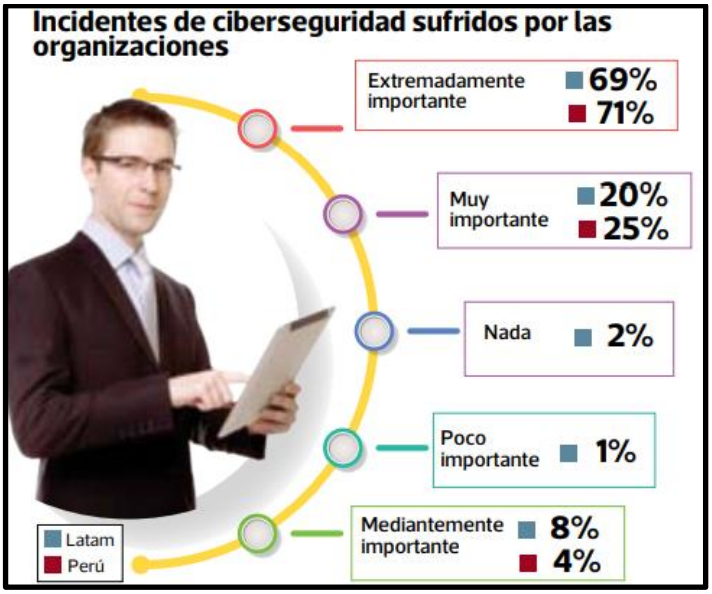


Figura 4. Incidentes de Ciberseguridad en el Perú

Fuente: https://www2.deloitte.com/

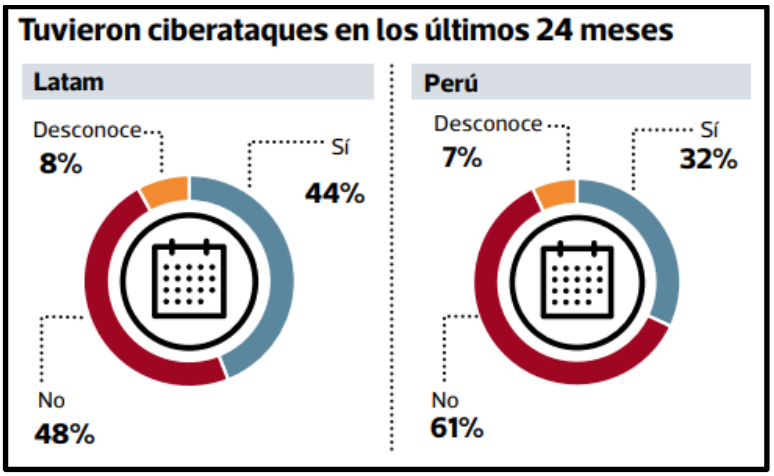


Figura 5. Estadística de Ataques en el Perú

Fuente: https://www2.deloitte.com/

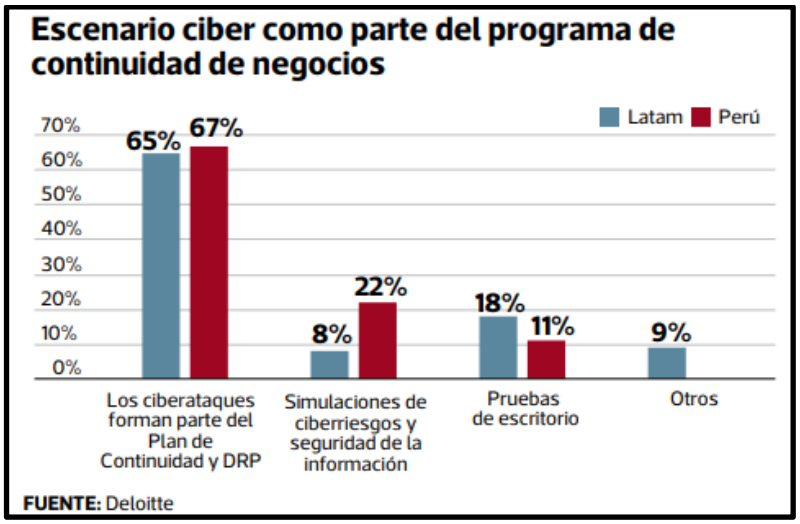


Figura 6. Escenarios de Continuidad del negocio en el Perú

Fuente: https://www2.deloitte.com/

Las compañías peruanas consultadas se consideran medianamente protegidas en ciberseguridad (36%), un 71% de las corporaciones considera extremadamente importante aplicar medidas y solo un 4% que no es relevante.

Se realizó una encuesta de conocimiento a los colaboradores donde se evidenció que el 50% no tiene conocimiento de cómo se realiza un plan de contingencia.

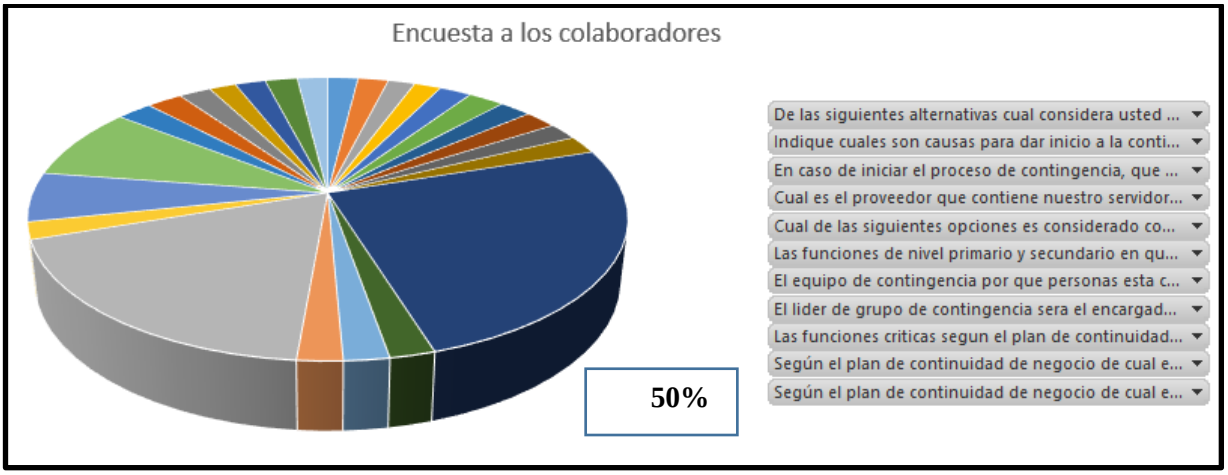


Figura 7. Encuesta a los colaboradores la Fiduciaria

Fuente: Recuperado de la Base de datos de la Fiduciaria.

Caracterización del área en que se participó

La Fiduciaria se encuentra en un proceso de renovación y mejora de su Infraestructura Tecnológica (Servidores) cómo mecanismo de respaldo de sus servicios más críticos para la compañía.

La Fiduciaria ha decidido desplegar una nueva Arquitectura de Servicios en Tecnología de la Información (IT) con un sistema de integración y replicación constante para asegurar la seguridad de su información y servicios.

La solución que se va implementar dentro de la empresa permitirá tener un soporte a las soluciones tecnológicas que requiera. Por tal motivo es importante poder alinear la infraestructura TI a las necesidades de nuevos procedimientos y niveles de SLA. Permitiendo ofrecer mejores niveles de servicios. Permitiendo generar un alto grado de satisfacciones de los usuarios de la empresa. Además de generar un crecimiento a futuro por parte de la empresa.

Esta nueva tecnología consiste en la integración de los productos Microsoft Azure, CloudBerry y Carbonite, los cuales permitirán a la compañía, asegurar sus servicios y contar con un sitio de respaldo desde la nube para continuar con sus actividades como compañía.

El área de Sistemas y encargada del desarrollo del proyecto estará conformada por dos analistas de sistemas y un consultor de Microsoft Azure.

Estadísticas

E.Y. en su encuesta global de seguridad y continuidad de servicios indica que:

El 9% de empresas cuenta con una función encargada de coordinar los riegos cítricos. Los más importantes son: eficiencia y productividad, contingencias legales, seguridad y salud, mercado y selección y ejecución de la estrategia.

El 58% de empresas reconoce que es importante fortalecer la cultura organizacional, seguida por la Necesidad de optimizar sus procesos mejorar sus procedimientos y políticas de seguridad.

El 83% de las empresas financiera manifestó tener un control de auditoria interna. De este grupo, el 82% indicó haberla constituido con recursos propios, mientras que el 18% restante, de manera tercer izada

Dentro de los estándares, de mejores prácticas y marcos metodológicos más implementados en las entidades bancarias de la región, se encuentran las normas ISO 22301 y COBIT (en el 68% y 50% de las entidades bancarias, respectivamente).

El 37% de entidades financiera indicaron que fueron víctimas de incidentes, y el principal propósito de estos ataques fueron los motivos económicos, un 79% de entidades financieras fueron víctimas de este ataque.

El 49% de las entidades financieras no implementan procesos con tecnología digital emergente, como big data, machine learning. Las cuales son fundamentales para que las organizaciones puedan prevenir ataques informáticos o determinar ataques sospechosos de sabotaje de información.

Estadísticas de sistemas, controles y procesos implementados en entidades financieras de Latinoamérica:

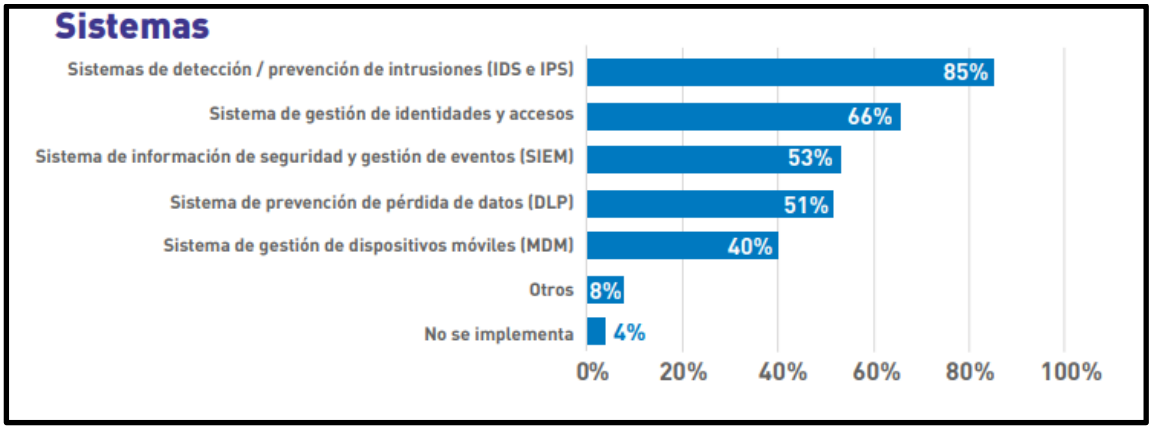


Figura 8. Estadísticas de Sistemas de Entidades

Fuente: Encuesta global de seguridad y continuidad de servicios Recuperado de www.ey.com

Figura 9. Estadísticas de Procesos de Entidades Financieras
Fuente: Encuesta global de seguridad y continuidad de servicios Recuperado de www.ey.com

E.Y. indica que a nivel global los bancos que están invirtiendo o comenzando a invertir en nuevas tecnologías en los próximos tres años están adoptando múltiples enfoques para incorporar las capacidades de las tecnología, la inteligencia artificial, cloud computing y la analítica avanzada desempeñarán un papel clave en la prevención de los ciberataques y poder contar con un adecuado plan de contingencia.

Análisis FODA

Fortalezas

- Variedad de herramientas de replicación y backup en tiempo real
- Equipo de trabajo especializado en TI
- Predisposición para la mejora continua de la empresa
- Variedad de herramientas de cloud computing

Oportunidades

- Oportunidad de adoptar nuevas tecnologías.
- Oportunidad de poder contar con una tecnología que permitirá generar ahorro en los próximos años.
- Oportunidad de poder tener un adecuado plan de continuidad del negocio y poder operar en cualquier parte del territorio nacional.

Debilidades

- No poder contar con un adecuado plan del proyecto.
- Transición con la adopción de la tecnología en la nube.
- No invertir en Cloud Computing

Amenazas

- Ataques informáticos (Hacking).
- Caída de los servicios de internet, esto imposibilita poder conectarse con la nube.
- Pérdida Financiera en el futuro.

Diagrama Causa – Efecto (Ishikawa)

Se desarrolló un diagrama de Ishikawa donde se muestra los principales factores de un deficiente plan de continuidad de los servicios de TI

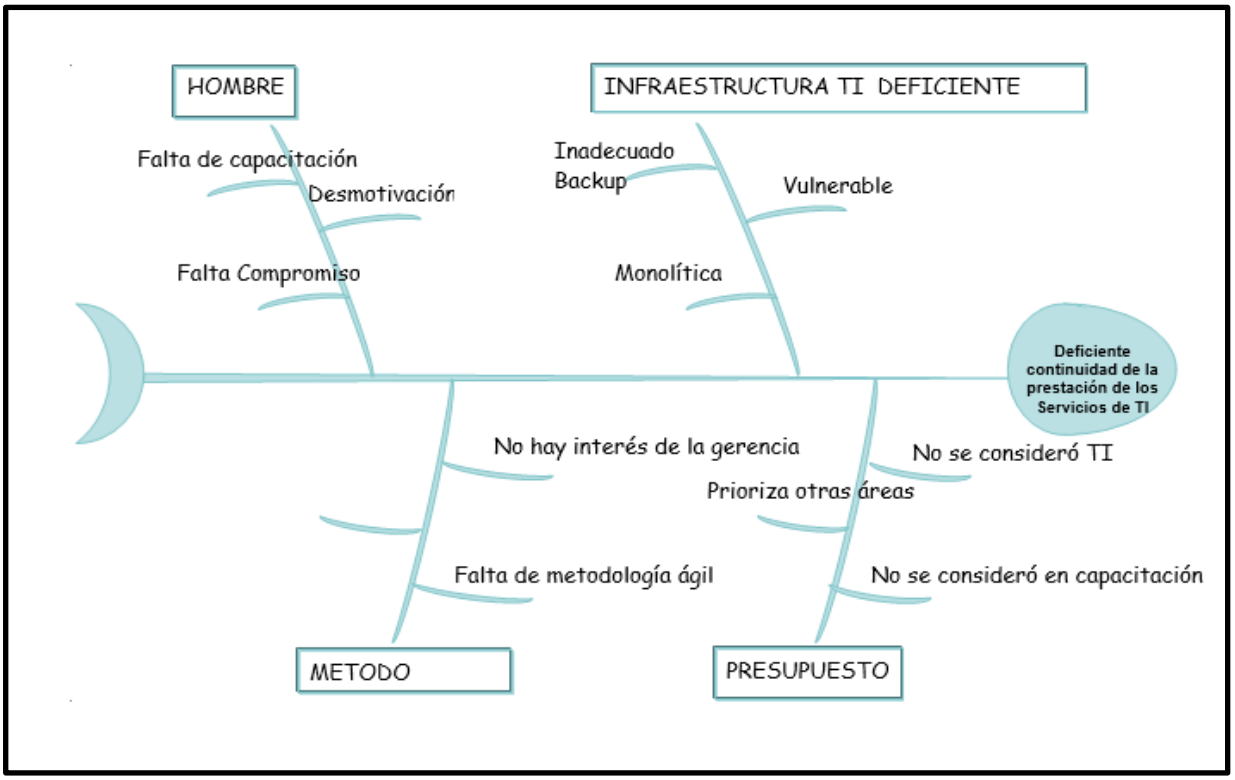


Figura 10. Diagrama Ishikawa de la Fiduciaria
Fuente: Elaboración Propia

Actualmente la empresa maneja una infraestructura la cual permite operar el giro del negocio, luego de realizar el diagrama de Ishikawa se pudo identificar 2 principales problemas:

Falta de Capacitación:

No se cuenta con una adecuada capacitación con nuevas herramientas de tecnología y plan de continuidad, que permita poder estar alineados a las nuevas tendencias en soluciones tecnológicas.

Inadecuado Backup:

La información que maneja la empresa ha ido incrementando en los últimos años, esto implica que los ataques informáticos y robo de información puedan vulnerar los sistemas que maneja la empresa actualmente. Se necesita mejorar e implementar nuevas herramientas de backup que permita contrarrestar estas vulnerabilidades.

Diagrama de Pareto

Se recolecto los principales incidentes que pueden generar un mal plan de continuidad de los servicios:

Tabla 1.

Cuadro de Incidencia y Frecuencia Acumulada

Incidentes	Frecuencia	Porcentaje	% Frecuencia Acumulada
No cuenta con un adecuado plan de continuidad	30	34%	34%
No cuenta con capacitación plan de contingencia	20	23%	57%
No cuenta con capacitación de seguridad de información	20	23%	80%
No cuenta con capacitación en cloud	2	2%	83%
Maneja data sensible	15	17%	100%
Total	87	100%	

Nota. Incidentes críticos. Tomado del cuestionario de Seguridad del área de sistemas de la Fiduciaria http://www.lafiduciaria.com.pe/

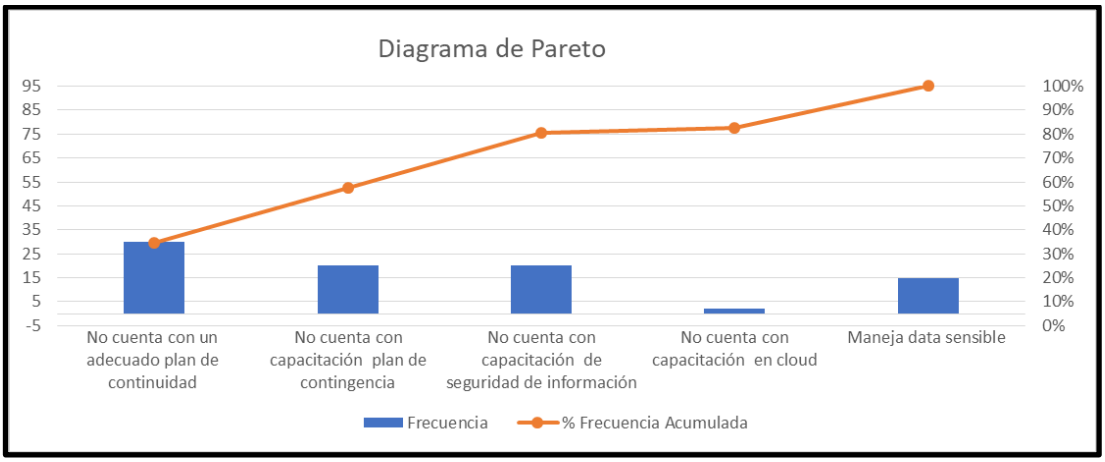


Figura 11. Diagrama de Pareto

Fuente: Elaboración Propia

Se identificó que al 80% los principales eventos son respecto a que no se cuenta con un adecuado plan de continuidad de los servicios de la empresa.

Antecedentes del problema

La Fiduciaria siendo un ente financiero que maneja mucha información, se identificó que no cuenta con un adecuado plan de contingencia ante algún desastre o hecho que detenga la operatividad del negocio, lo que resulta un gran problema a nivel de imagen institucional.

En la actualidad las compañías, grandes o pequeñas, depositan su activo más preciado en sistemas informáticos, sin embargo, son muy pocas las que implantan un adecuado plan de continuidad de los servicios con ayuda de la nube, que permita un adecuado levantamiento de las operaciones de la organización.

Se identificó que no es suficiente contar con un poderoso antivirus o mantener un backup diario de la información pensando que eso mantendrá segura la información, sino es necesario contar con procedimientos y herramientas alternativos que permitan ante alguna contingencia mantener la continuidad de los servicios de la empresa. Dentro de estos procedimientos alternativos se implementará las herramientas de Microsoft Azure que permitirá poder contar con la tecnología en la nube para tener un adecuado plan de continuidad de la empresa.

Definición del Problema

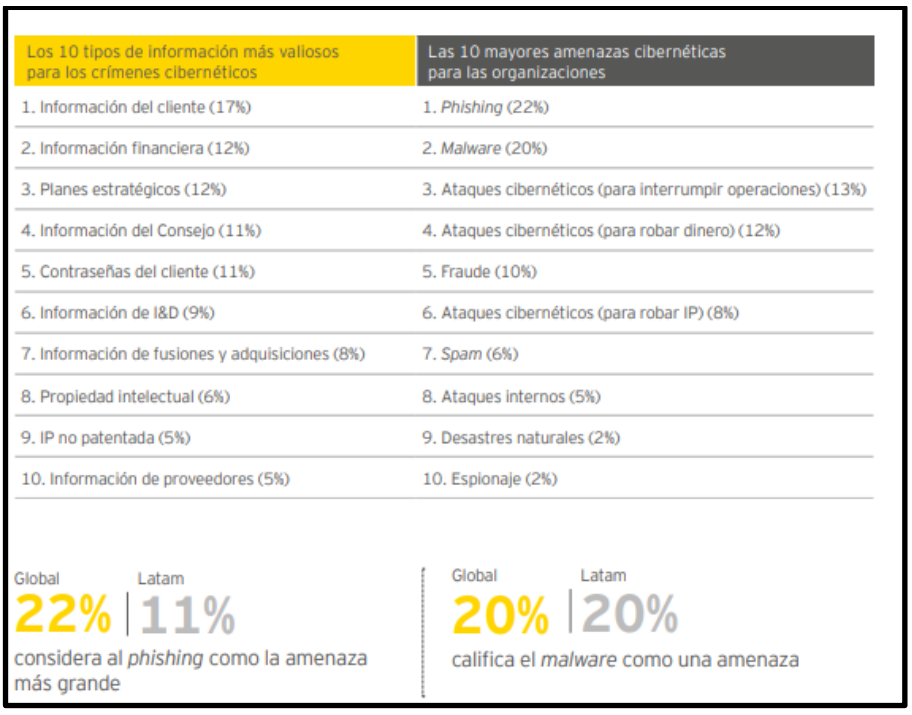
De acuerdo con la última auditoría realizada el 14-06- 2017 a la empresa La Fiduciaria se identificó las siguientes vulnerabilidades que afectan el desarrollo del negocio.

No se cuenta con una solución tecnológica que permita asegurar la continuidad operativa de manera, ágil, rápida y sencilla, sin necesidad de adquirir más infraestructura física que se tenga que mantener y soportar en el centro de datos.

No se realiza pruebas de penetración y evaluaciones de vulnerabilidades independientes.

Mejorar los procedimientos internos (Políticas, manuales), no se cuenta con un adecuado plan de continuidad del negocio y recuperación después de desastres.

E.Y. en su encuesta de seguridad de la información del 2018 presenta las principales vulnerabilidades y amenazas.



Los 10 tipos de información más valiosos para los crímenes cibernéticos	Las 10 mayores amenazas cibernéticas para las organizaciones
1. Información del cliente (17%)	1. *Phishing* (22%)
2. Información financiera (12%)	2. *Malware* (20%)
3. Planes estratégicos (12%)	3. Ataques cibernéticos (para interrumpir operaciones) (13%)
4. Información del Consejo (11%)	4. Ataques cibernéticos (para robar dinero) (12%)
5. Contraseñas del cliente (11%)	5. Fraude (10%)
6. Información de I&D (9%)	6. Ataques cibernéticos (para robar IP) (8%)
7. Información de fusiones y adquisiciones (8%)	7. *Spam* (6%)
8. Propiedad intelectual (6%)	8. Ataques internos (5%)
9. IP no patentada (5%)	9. Desastres naturales (2%)
10. Información de proveedores (5%)	10. Espionaje (2%)

Figura 12. Estadística de Vulnerabilidades y Amenazas de Información

Fuente: Encuesta de ciberseguridad de la información Recuperado de www.ey.com

Lo que se busca mejorar en la empresa es:

- La Falta de coordinación entre las jefaturas y gerencia con relación a mejorar el plan de continuidad de la empresa, esto genera que los tiempos de reanudación de los servicios sigan siendo elevados.
- El desconocimiento de la tecnología y beneficios de la nube por parte de la gerencia.
- La Falta de capacitaciones a la gerencia en cuanto a nuevas tecnologías de la nube para mejorar el plan de continuidad de los servicios.
- Los servidores no cuentan con un respaldo en la nube de la totalidad de sus servicios principales en caso ocurriera un desastre o incidente sobrenatural.

Implicación y Riesgo:

Riesgo Tecnológico/Operativo

- El riesgo tecnológico puede verse desde tres aspectos, primero a nivel de la infraestructura tecnológica (hardware o nivel físico), en segundo lugar a nivel lógico (riesgos asociados a software, sistemas de información e información) y por último los riesgos derivados del mal uso de los anteriores factores, que corresponde al factor humano como un tercer nivel.

- Si bien atender el fenómeno de la digitalización constituye una prioridad competitiva clave para las organizaciones, las organizaciones no logran hallar un punto de partida claro para implementar iniciativas;

- El foco de la digitalización aún se centra en beneficios tácticos (ej: reducción de costos, de plantilla y de costos operativos de procesos).

- En relación al año 2016, las organizaciones están dejando de identificar restricciones / limitaciones en sus TICs como barrera frente a la digitalización; la complejidad, no obstante, subyace en decidir cómo emplear la tecnología para brindar soporte a iniciativas estratégicas.

- Las organizaciones requieren una visión centrada en la gestión como medio para optimizar los beneficios de la digitalización, así como también, las habilidades necesarias para capitalizarlos internamente.

Indisponibilidad prolongada de servicios de TI

Explotación de vulnerabilidades en servidores de bases de datos, así como modificaciones no autorizadas, lo cual podría originar pérdida de integridad de datos, fuga de información o pérdida de disponibilidad de los servicios/aplicaciones.

Objetivos:

General:

- Implementar la migración de los servidores a la nube a través de Microsoft Azure y sus herramientas colaborativas para contar con un plan de continuidad de los servicios de TI en la empresa La Fiduciaria, Lima 2018.

Específico:

- Reducir el tiempo de recuperación de la infraestructura tecnológica incluyendo como criterio de éxito la reanudación de las funciones primarias en por lo menos 24 horas o menos. Actualmente se demora 72 horas.
- Provisionar una nube privada virtual integrada a la red de la Fiduciaria, a través de un túnel VPN. Actualmente se cuenta solo con un repositorio de almacenamiento en la nube.
- Poder contar con servidores a demanda sobre la infraestructura Cloud para utilizar el Recovery programado en tiempo real. Actualmente no se cuenta con servidores de respaldo en la nube.
- Crear una réplica continua de los servidores primarios en los servidores de contingencia. Actualmente no se cuenta con replicación en tiempo real.
- Realizar las buenas prácticas de gestión que deben tener las empresas al adoptar la tecnología en la nube, para obtener y mejorar en la prestación de los servicios TI. Actualmente no se realiza charlas plan de continuidad del negocio.
- Realizar una evaluación económica del proyecto.

Justificación

La Fiduciaria al ser una entidad financiera esta normada bajo la circular G-140 de la SBS, que está bajo los estándares de la ISO 27001 (seguridad de la información), que es una norma internacional que describe como tener una correcta gestión de la información que es uno de los activos más importantes de una empresa, proporciona una metodología de gestión enfocada en seguridad de la información.

Es importante contar con lo último en tecnología para poder ser una empresa competitiva hace que se tenga que implementar nuevas herramientas de tratamiento y cuidado de la información ante cualquier evento desafortunado que pueda interrumpir las operaciones del negocio.

Los sistemas basados en la nube han surgido en los últimos años y se han convertido en una herramienta, ya que los proveedores de dichos servicios, han invertido en tecnologías avanzadas para la protección de datos, privacidad, conectividad segura y un mejor control de accesos. Para la mayoría de los encuestados, estos servicios sirven para proteger los datos sensibles y reforzar la privacidad, incluyendo el monitoreo y análisis en “real time” de posibles vulnerabilidades, y comportamientos anómalos, entre otros.

Compartir información e implementar tecnologías avanzadas de ciberseguridad no va a detener todos los ciber ataques o amenazas. Muchas empresas ya cuentan con soluciones en la nube que permite tener un mejor control de sus sistemas y servicios.

Otro punto importante a destacar si no se cuenta con un adecuado plan de continuidad es que los ataques de seguridad informática producen daños que afectan a toda la empresa, ya sea en las operaciones, reputación y, por lo tanto a los ingresos.

Sobre la implementación de los servidores en la nube, permitirá poder tener un adecuado plan de continuidad ante cualquier ataque o desastre que se pueda presentar en la empresa. Se ejecutará en el plazo y tiempo ideal para que no afecte la operatividad del negocio.

Alcances

- El proyecto de migración de la infraestructura en la nube abarcará el área, los servidores Core de la empresa (DataFile, Direcotrio, Bases de Datos).
- Se examinará los sistemas core y los servicios críticos, brindando los 3 pilares de la seguridad que son integridad, confidencialidad y confiabilidad dentro de la empresa.
- Se comprobará el correcto funcionamiento de los sistemas y servicios TI alojadas en la nube.

- La migración no interrumpirá las operaciones de la empresa.

Limitaciones

- Tiempo limitado para el desarrollo del proyecto, ya que la empresa cuenta con auditorias constantemente.
- La nube necesita un ambiente con conexión a internet para poder restaurar los servicios de la empresa.

Capítulo III: Marco Teórico

Computación en la nube

Arana, L., Ruiz, M., Serna, N., P (2015).Análisis de aplicaciones empleando la computación en la nube de tipo PaaS y la metodología scrum, *Revista de la facultad de ingeniería Industrial, 18,*159-160

Nos dicen:

La tecnología Windows Azure como servicio (PaaS), es importante por dos razones principales: la primera es que la programación .net se supo acoplar sin ninguna dificultad y segundo la base de datos sql de azure presenta una interfaz amigable y de fácil uso para el usuario final.

Computación en la nube como paradigma

Valera, C., Portella, J., Pallares, L., P. (2016). Computación en la nube: un nuevo paradigma en las tecnologías de la información y la comunicación, *Revista de ingeniería industrial* ,144-145.

Nos dicen:

La nube proporciona acceso a los diferentes usuarios individuales para cada recurso de información, de forma ágil, dinámica y económica. Asimismo las empresas pueden sistematizar todos sus procesos de una forma más eficiente. Esto permite poder reducir los costos en inversión de equipos y software. Estos costos de inversión son trasladados a los costos de operativos. Los costos de la nube son considerados como servicios por demanda de forma mensual.

Gestión del conocimiento en la nube

Trujillo, M., Marulanda, C., Vega, O., P (2011), Servicio de Gestión de Conocimiento Utilizando la Computación en Nube, *Entre ciencia e Ingeniería, 9,182*-183

Nos dicen:

Desde que empezó a desarrollarse la tecnología en la nube, está permitiendo poder ser implementadas en las TIC de las empresas generando una mayor capacidad de integrar aplicaciones y el trabajo colaborativo.

Toda empresa que desee avanzar en las nuevas tecnologías de la gestión del conocimiento para su desarrollo empresarial debe utilizar las nuevas tendencias como (cloud computing, servicios de web social, etc.).

Cloud Computing y su desarrollo de servicios:

Según Zhang (2016), en su artículo, Cloud computing y su desarrollo de servicios:

Nos menciona que:

Después de las aplicaciones de cloud computing, los usuarios no deben preocuparse por la compra de software, el mantenimiento y las actualizaciones, estos trabajos se completarán con cloud computing. Según, La Revista Ibérica de Sistemas y Tecnologías de la Información presenta artículos actuales sobre los principales temas de la especialización de revistas para abordar y enfocar la extracción de datos y la tecnología relacionada en las tecnologías de la información (P.5).

Plataforma Microsoft Azure

Azure nos ayuda a afrontar los desafíos empresariales más difíciles. Azure proporciona más de 100 servicios que permiten hacer todo tipo de cosas: desde ejecutar aplicaciones en máquinas virtuales hasta explorar nuevos paradigmas de software, como bots inteligentes y realidad mixta.

En definitiva, la informática en la nube le permite alquilar eficacia de proceso y almacenamiento en lugar de comprar recursos físicos, como unidades CPU y almacenamiento. Azure, administra los activos físicos por usted, para que pueda dedicar menos tiempo a la infraestructura y centrarse más en compilar una nueva aplicación sensacional.

Pero Azure es mucho más que un centro de datos distribuidos. Azure proporciona muchas clases de servicios que van bastante más allá de lo que puede hacer con hardware y software estándar. Estos servicios incluyen desde el análisis de macrodatos hasta la capacidad para comunicarse de forma natural con los usuarios.

El acceso a la infraestructura y a los servicios en Azure le permite entregar rápidamente características nuevas e innovadoras a sus usuarios. Los proyectos que antes tardaban meses ahora suelen completarse en semanas o días.

Cloud Computing

"El cloud computing es una tecnología que consiste en tener una arquitectura de prestación de diferentes servicios de tecnología de información. Esta tendencia está adquiriendo protagonismo en estos últimos años.” (Mir Alies, 2010).

Modelos de Servicio

Microsoft ofrece impresionantes servicios en la nube basados en sus productos de software locales ampliamente utilizados.

Windows Azure es IaaS y PaaS, lo que hace que el sistema operativo Windows Server y otras características estén disponibles como servicios.

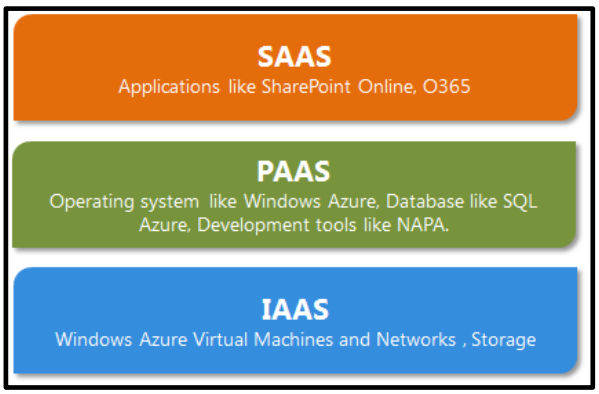


Figura 13. Modelo de Servicios
Fuente: Recuperado de https://azure.microsoft.com

Infraestructura como servicio (IaaS)

Al usar Microsoft Windows Azure, puede configurar nuevas máquinas virtuales Windows Server y Linux y ajustar su uso a medida que cambien sus requisitos. Solo tienes que pagar por el servicio que utilizas. A continuación, se muestra una imagen de los servicios de Windows Azure desde el portal.

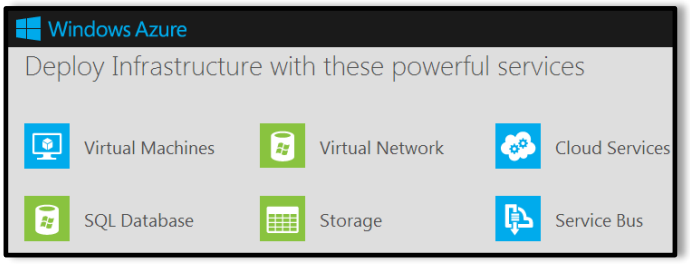


Figura 14. Catálogo de Servicios
Fuente: Recuperado de https://azure.microsoft.com

Uno de los mayores beneficios de IaaS es que proporciona control granular, donde puede elegir los componentes principales para su infraestructura. Al agrupar sus recursos de computación y almacenamiento, puede escalar con facilidad y rapidez para satisfacer las necesidades de infraestructura de toda su organización o departamentos individuales, global o localmente.

Escenarios IaaS

Las aplicaciones web IaaS permiten que toda la infraestructura de TI pueda soportar cualquier aplicación web, incluidos servidores de almacenamiento y recursos de red. Las organizaciones pueden implementar rápidamente aplicaciones web en IaaS y escalar fácilmente la infraestructura cuando la demanda de las aplicaciones es impredecible.

Computación de alto rendimiento, ayuda a resolver problemas complejos que involucran millones de variables o cálculos. Los ejemplos incluyen simulaciones de terremoto y plegamiento de proteínas, predicciones climáticas y climáticas, modelos financieros y evaluación de diseños de productos.

Análisis de grandes datos. Big data es un término popular que contienen patrones, tendencias y asociaciones potencialmente valiosos. Los conjuntos de datos de minería para ubicar o eliminar estos patrones ocultos requieren una gran cantidad de potencia de procesamiento, que IaaS proporciona económicamente.

Plataforma como servicio (PaaS)

Microsoft Windows Azure PaaS se puede utilizar como un entorno de desarrollo, alojamiento de servicios y gestión de servicios. SQL Azure puede proporcionar servicios de datos, incluida una base de datos relacional, informes y sincronización de datos. Tanto

Windows Azure como SQL Azure son los componentes clave de la plataforma en la nube de Azure. Con esta plataforma, puede concentrarse en implementar sus aplicaciones personalizadas y puede configurar fácilmente sus aplicaciones para ampliarlas o reducirlas a medida que cambien las demandas.

La plataforma Microsoft Azure como PaaS puede admitir diferentes roles, como Worker y Web. Por ejemplo, puede ejecutar aplicaciones web con el rol web, así como hospedar aplicaciones de nivel medio, como Workflow, en el rol de trabajador. De manera similar, SQL Azure proporciona el motor de base de datos relacional central de Microsoft como un servicio de plataforma.

Uno de los beneficios clave de PaaS es que no debe preocuparse por el funcionamiento del sistema operativo o las actualizaciones (paquetes de servicio) y las actualizaciones de hardware. El Proveedor revisa regularmente su sistema operativo, actualiza las características de la plataforma (como la plataforma .NET central o el motor de base de datos SQL) y actualiza el hardware a pedido para satisfacer su demanda.

Escenarios PaaS

Las organizaciones suelen utilizar PaaS para estos escenarios:

Proporciona un marco que los desarrolladores pueden desarrollar o personalizar aplicaciones en la nube. Similar a la forma en que creas una macro de Excel, PaaS permite a los desarrolladores crear aplicaciones utilizando componentes de software integrados. Se incluyen funciones en la nube, como la capacidad de ampliación, alta disponibilidad y capacidad para múltiples inquilinos, lo que reduce la cantidad de codificación que deben hacer los desarrolladores.

Analítica o inteligencia empresarial. Las herramientas proporcionadas como un servicio con PaaS permiten a las organizaciones analizar y extraer sus datos, encontrar perspectivas y patrones y predecir resultados para mejorar el pronóstico, las decisiones de diseño de productos, los retornos de inversión y tomas de decisiones.

Ventajas

Azure es una herramienta que cuenta con soluciones en la nube, ofreciendo una serie de ventajas. Con las siguientes características.

Disponibilidad

Azure ofrece niveles de servicio con una disponibilidad del 99.95%, resultando ser de mucha importancia para los sistemas y servicios críticos de las empresas. Evitando así la caída de los mismo que podría generar grandes pérdidas económicas, físicas. Sin ser una situación grave los usuarios reportaran rápidamente cualquier caída de aplicaciones. Azure ofrece alta redundancia de servidores gracias a sus niveles de servicio.

Escalabilidad

Toda empresa tiene diferentes necesidades y requerimientos, y pueden llegar a variar a lo largo del tiempo por diversos factores, por la tendencia de las nuevas tecnologías.

Azure ofrece esa capacidad de poder ampliar o reducir en función a las necesidades de cada empresa. Y solo se paga por lo que se va utilizar. Esto permite poder agregar más recursos en función a la demanda.

Versatilidad

Como se ha explicado azure, permite ser abierto y flexible a cualquier necesidad o requerimiento y no solamente al entorno Microsoft. Y está abierto a al desarrollo de cualquier lenguaje y sobre cualquier framework.

Ubicuidad

Azure posee un gran marco territorial y está ubicado en 24 regiones de todo el mundo que contiene una red mundial de centro de datos.

Servicios de Microsoft Azure

Los servicios de Microsoft Azure están orientados al crecimiento y desarrollo empresarial, es decir todos los servicios que ofrece son escalables y se amoldan a las necesidades más particulares de cualquier empresa.

Azure ofrece un amplio portafolio de servicios los cuales se describen a continuación: Almacenamiento:

Servicios Móviles: Azure permite la creación y desarrollo de aplicaciones para diferentes sistemas operativos de móviles.

Herramientas de seguridad: Azure ofrece diferentes protocolos y herramientas orientados a la seguridad de la información, protegiendo la información local o en la nube, como por ejemplo la creación de sistemas de autentificación, recuperación de desastres, copias de seguidad.

Flujos de trabajo: Azure ofrece diferentes tareas y procesos, como los procesos de automatización y optimización de flujos de trabajo y servicios complementarios.

Máquinas virtuales: Azure permite la creación, administración y gestión de máquinas virtuales con gran capacidad.

ISO 22301

La ISO 22301, es una norma que permite tener una adecuada gestión de continuidad del negocio, y puede ser utilizada por cualquier empresa.

Toda empresa que aplique los estándares de la ISO 22301, puede certificarse y demostrar que son capaces de poseer un adecuado plan de contingencia basado en las buenas prácticas.

La norma centra sus objetivos en 4 actividades principales que se muestran a continuación:

- Saber las necesidades y requerimientos de las empresas para establecer políticas y objetivos para una adecuada gestión de la continuidad del negocio.
- Saber implantar controles para la gestión de incidentes dentro de una organización.
- Tener un seguimiento y revisión del desempeño del SGCN.
- Implementar mejora continua basada en mediciones objetivas.

Para Duch, (2016) En su artículo *Las empresas frente a las amenazas externas*
Nos dice:

Actualmente, la norma ISO se ha convertido en un referente para la aplicación de políticas de gestión de continuidad de los servicios de tal forma que un 51% de las empresas que implementan esta gestión se basan en la ISO 22301. Aquellos sectores en los que hay una mayor penetración de la norma son el sector IT/telecomunicaciones (66%), el sector de servicios profesionales (56%) y el sector financiero (53%).Si bien esta norma se centra en las necesidades que deben tener un adecuado sistema de continuidad del negocio, no establece cómo debe implementarse el sistema. De esto se ocupa la norma 22313, que fija las directrices para la implantación de un sistema de continuidad del negocio y que complementa a la norma 22301.

Para Planas, (2015) en su artículo *¿Necesitas un plan de Continuidad de negocio?*
Nos dice:

La información es uno de los activos más importantes para una organización, y que mediante una adecuada implementación de continuidad del negocio, se puede mantener el valor dentro de una organización. A su vez se crea una relación directa con las vulnerabilidades, protegiendo a la empresa de que puedan ocasionar la interrupción del servicio. Esto reduce la probabilidad que se produzcan caídas de los servicios.
La norma ISO nos brinda un conjunto de principios para la tener una adecuada continuidad del negocio. Ofreciendo técnicas aprobadas por un órgano de normalización reconocido que permite poder medir una organización.

CAPÍTULO IV: DESARROLLO DEL PROYECTO

Introducción

La Fiduciaria se encuentra en un proceso de renovación y mejora de su Infraestructura Tecnológica cómo mecanismo de respaldo de sus servicios más críticos para la compañía.

La Fiduciaria ha decidido desplegar una nueva Arquitectura de Servicios en Tecnología de la Información (IT) con un sistema de integración y replicación constante para asegurar la seguridad de su información y servicios.

El desarrollo del proyecto tiene por objetivo proponer un modelo para mejorar la continuidad de los servicios de La Fiduciaria basada en la norma técnica internacional ISO 22301.

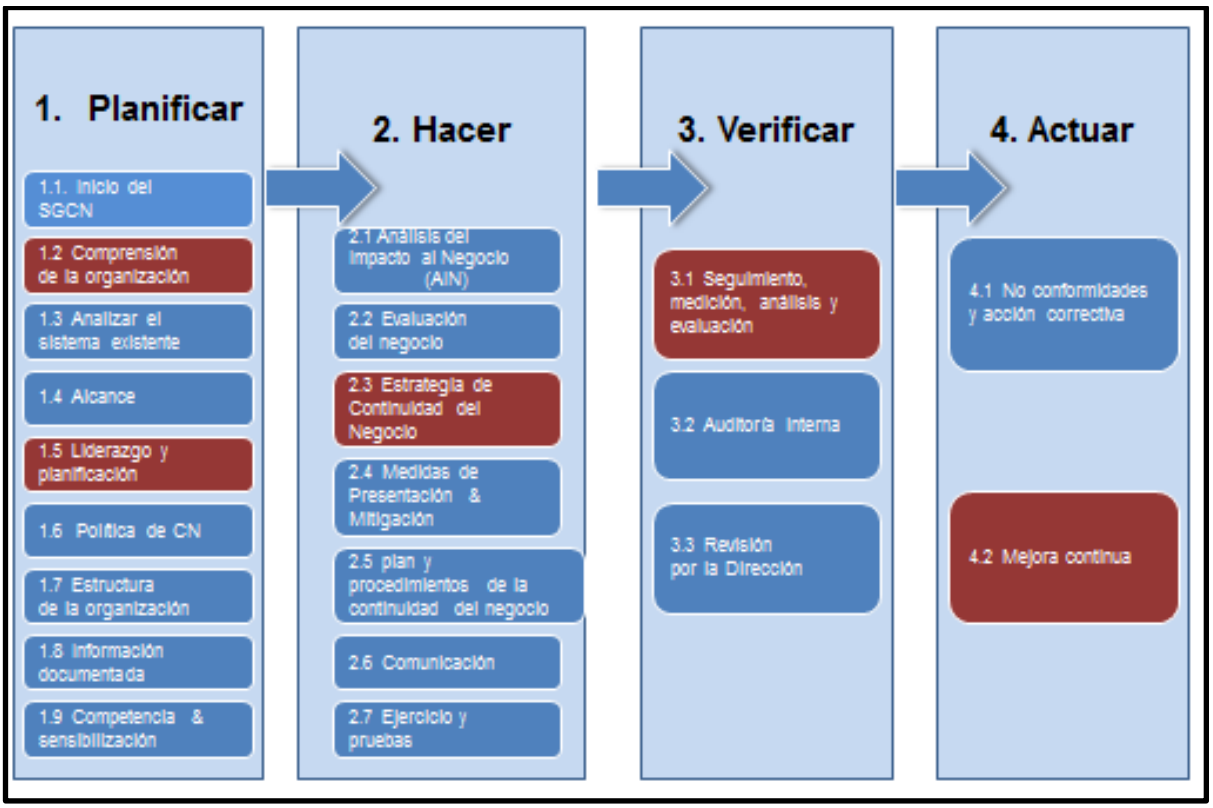


Figura 15. Marco Metodológico de la ISO 22301

Fuente: Elaboración propia

Dentro de la fase de planificación se escogieron las siguientes actividades:

Fase 1 Comprensión de la organización

En esta fase, se procede a realizar un análisis de los impactos financieros y operacionales de un desastre en la organización, sus áreas y procesos. Los impactos financieros son las pérdidas económicas a las que está expuesta la empresa, como son: pérdidas de ventas, penalidades contractuales o degradación de productos. Los impactos operacionales son pérdidas no económicas que guardan relación con las operaciones del negocio, como son: pérdida de competitividad, daño a la confidencialidad de inversión, deficiente servicio al cliente y daño a la reputación del negocio.

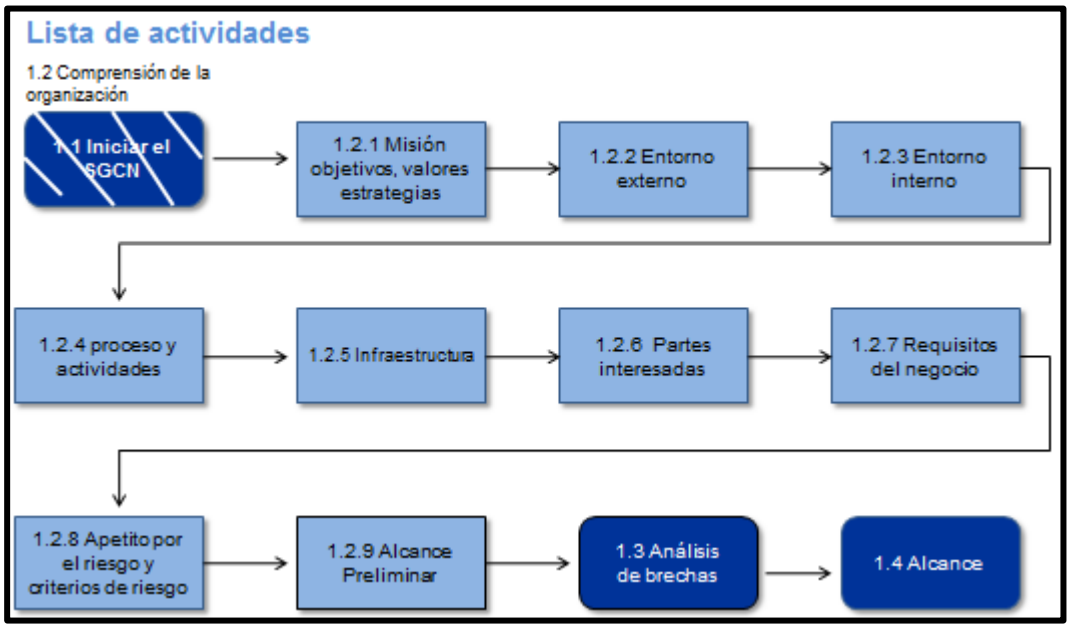


Figura 16. Actividades de Comprensión de la Organización

Fuente: Elaboración propia

Misión, Objetivos, Valores y Estrategias

- Proteger toda la información de la empresa de amenazas internas como externas para asegurar la alta disponibilidad de la misma.
- Asegurar el cumplimiento de las medidas de seguridad y plan de continuidad implementada en el procedimiento de contingencia de la empresa.
- Mantener actualizada y contar con un control de seguridad y de continuidad de la empresa.

- Administrar la seguridad de la información y establecer un marco gerencial para iniciar y controlar su implementación, así como la distribución de funciones y responsabilidades.
- Consulta con especialistas para obtener asesoramiento sobre materia de seguridad de la información.
- Aplicar medidas de seguridad para los accesos a los aplicativos e información por parte de terceros.
- Revisar y proponer soluciones sobre lo seguridad de la información que los gerentes deberán dar su aprobación.
- Monitorear cambios significativos en los riesgos que pueden afectar a la información de la empresa.
- Investigar y monitorear los incidentes relativos a la seguridad de la información.
- Aprobar nuevas metodologías y procesos para incrementar la seguridad de la información.
- Implementar controles para los sistemas de seguridad de la información.
- Promover la difusión de la seguridad de la información a todos los empleados de la empresa.

Entorno Externo

Cualquier elemento contingente en el área de sistemas afecta a todas las áreas de la oficina por lo que se deben tomar las medidas correctivas inmediatas. Para ello es importante que se pueda identificar los factores externos que puedan ocasionar una contingencia.

Tabla 2.

Criterios de Impacto y Escenarios

Causas	Escenario
• Incendio • Sabotaje • Sismos • Catástrofe General	Destrucción de la Sala de Servidores
• Falla de componentes de hardware o software de un servidor • Virus	Falla de un servidor

• Corte de energía eléctrica	Paralización total de las operaciones
• Falla de elementos de red (switches, o cableado).	Ausencia de red o conectividad.
• Falla de la línea dedicada	Ausencia de Internet y correo electrónico.

Nota. Servicios críticos. Tomado de la política de seguridad del área de sistemas de la Fiduciaria http://www.lafiduciaria.com.pe/

Cualquier elemento contingente en el área de sistemas afecta a todas las áreas de la oficina por lo que se deben tomar las medidas correctivas inmediatas. Para ello es importante que se defina un equipo que sea el que ejecute el Plan de Contingencia que puede estar constituido por el personal de soporte de la empresa en primer lugar por personal de otras áreas en el caso de que la contingencia sea mayor.

Identificación de Riesgos

Se deben considerar las amenazas, vulnerabilidades y escenarios de riesgos que puedan interrumpir la continuidad del negocio. Una amenaza es un factor externo que podría ocasionar la ocurrencia de un riesgo en una organización o empresa.

Las amenazas pueden ser:

Amenazas Naturales: son aquellas que se originan por desastres o fenómenos naturales.

Por ejemplo: lluvias, derrumbes, inundaciones, sismos, tormentas eléctricas.

Amenazas Humanas: son aquellas que son originadas por el hombre.

Por ejemplo: fuga de información, ataques informáticos, robo, fraude.

Amenazas Técnicas: son aquellas que se originan por una falla técnica.

Por ejemplo: fuego interno, deterioro de recursos, aniego, variación de energía eléctrica.

Una vulnerabilidad es un punto débil en la empresa que permite la ocurrencia de riesgos; es decir, la ausencia o debilidad en los controles.

Por ejemplo, las vulnerabilidades pueden estar relacionadas con la falta de capacitación del personal clave, ausencia de controles de acceso físico y ambiental a las instalaciones, infraestructura de red y comunicaciones insuficiente, infraestructura física no adecuada para eventuales desastres naturales, ausencia de medidas de prevención, entre otros.

Tabla 3.

Matriz de Evaluación de Riesgos y Nivel de Criticidad

DEPARTAMENTO	SERVICIO DE TI	CRITICIDAD
Financiero	Microsoft Office	Media
	Servidor de Archivos	Alta
	Bases de datos	Alta
	Aplicativos Core Bancario	Alta
	Aplicativos Financieros	Alta
	Aplicativos de gestión externa	Alta
	Mesa de Servicios	Media
	Conexión de red	Alta
	Carpetas compartidas	Baja
	Impresoras, copiadoras	Media
	Internet	Media
	Videoconferencia	Baja
	Telefonía fija	Media
Negocios	Microsoft Office	Media
	Servidor de Archivos	Alta
	Aplicativos Core Bancario	Alta
	Aplicativos de gestión externa	Alta
	Mesa de Servicios	Media
	Conexión de red	Alta
	Impresoras, copiadoras	Baja
	Internet	Media
	Videoconferencia	Media
	Telefonía fija, móvil	Alta
Tecnología	Microsoft Office	Media
	Aplicativos de monitoreo	Alta
	Aplicativos Tecnológicos	Alta
	Mesa de Servicios	Media
	Conexión de red	Alta
	Impresoras, copiadoras	Baja

Nota. Clasificación de servicios críticos. Tomado de la política de seguridad del área de sistemas de la Fiduciaria http://www.lafiduciaria.com.pe/

Entorno Interno

Líder de contingencia

Será la cabeza del grupo y es quien realizará las coordinaciones con los demás miembros del mismo y supervisará la ejecución del plan. Debe ser una persona con poder decisión y que sepa trabajar bajo presión. En principio será el encargado de los sistemas de la empresa que asumirá el liderazgo de la contingencia considerando su conocimiento amplio de cada uno de los componentes de hardware y software así como de las características de los sistemas de la empresa.

- Deberá supervisar que el Plan de Contingencia sea actualizado adecuadamente el cual debe ser revisado semestralmente.
- Será el responsable de que las medidas de seguridad dentro del área de sistemas se cumplan, llámese copias de respaldo, extintores, etc.
- Debe estar al tanto de que los contratos de garantía y mantenimiento de los equipos estén al día.

Personal de Soporte

Sera el área encargada del trabajo de reinstalación de los equipos y del software necesario que permitan reiniciar las actividades.

Infraestructura

Escenario Actual Infraestructura tecnológica de la fiduciaria

Actualmente la Fiduciaria cuenta con 6 servidores físicos en el centro de datos, y demora un promedio de 48 horas en restablecer los servicios core ante cualquier evento, afectando la operatividad del negocio.

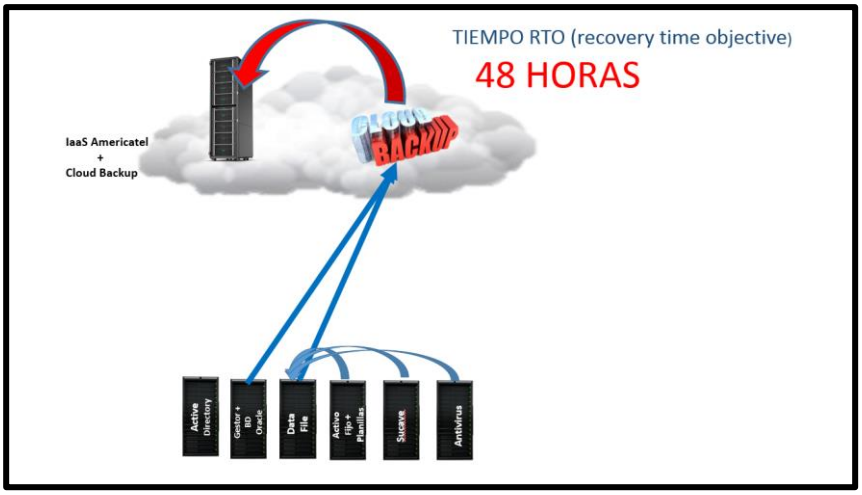


Figura 17. Infraestructura actual de la Fiduciaria

Fuente: Elaboración Propia

Escenario Esperado con la Migración de la Infraestructura tecnológica en la nube

Con la migración de los servidores en la nube de Microsoft Azure se espera que los servicios core de la Fiduciaria se inicien en un rango de 60 minutos como mínimo y máximo 5 horas permitiendo tener una infraestructura tecnológica integra para la continuidad de los servicio

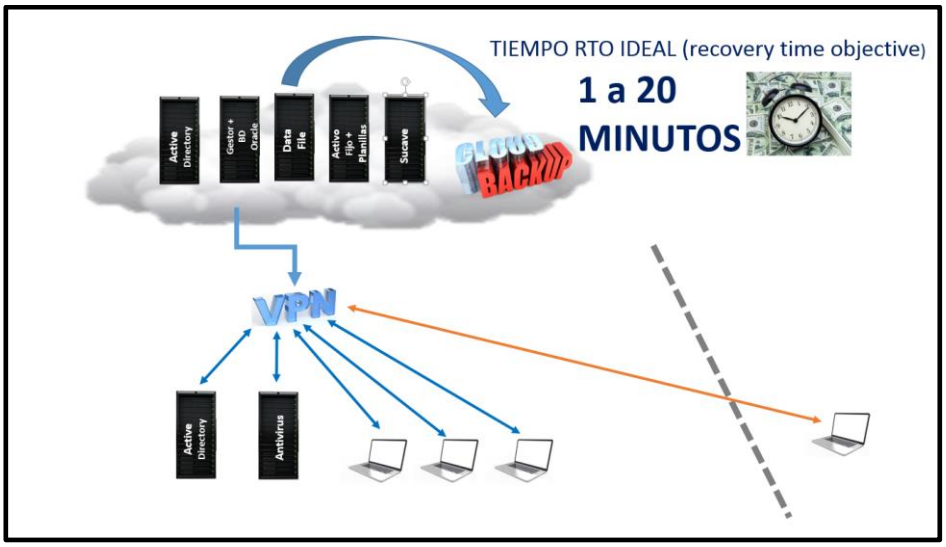


Figura 18. Infraestructura Esperada de la Fiduciaria

Fuente: Elaboración Propia

Fase 2 Liderazgo y Planificación

En esta fase se realiza la clasificación y responsabilidades del equipo de trabajo.

La gerencia deberá definir los requisitos, designar el personal encargado y coordinar el periodo del desarrollo del proyecto con el equipo de trabajo.

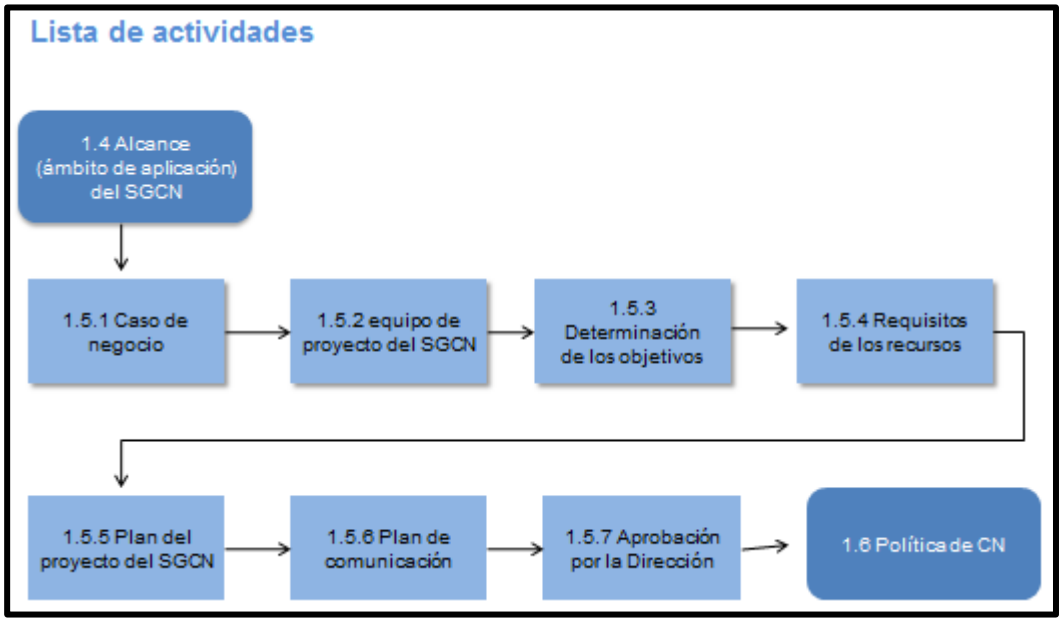


Figura 19. Actividades de Liderazgo y Planificación

Fuente: Elaboración propia

Equipo de proyecto del SGNCN

Estructura de Equipos:

Consultor de TI

- Estará a cargo de la ejecución de las actividades planificadas para el despliegue de la infraestructura como un servicio

Líder de Proyecto:

- Personal contratado por la empresa
- Encargado de gestionar el proyecto
- Facilitará las coordinaciones con las áreas internas y proveedores pertinentes según la necesidad de las actividades a ejecutar

Determinación de los Objetivos

Para poder llevar a cabo el desarrollo del proyecto se realizaron auditorías internas a la empresa durante el año 2018, y se optó poder mejorar los sistemas de información con una nueva solución basada en la tecnología del cloud computing utilizando los servicios de Microsoft Azure como principal aliado, y así poder tener un mejor manejo y control de los sistemas core de la empresa.

- Contar con una solución tecnológica que le permita asegurar la continuidad operativa de manera ágil, rápida sencilla.
- No tener la necesidad de adquirir más infraestructura física a mantener y soportar en su centro de datos.
- Evitar los tiempos de adquisición, preparación y configuración de la infraestructura tradicional.
- Buscar mejores alternativas a una solución tradicional de recuperación ante desastres.

Plan del Proyecto del SGCN

- La solución creará una réplica continua de los servidores primarios en los servidores de contingencia.

- Cuando ocurre una falla, los servidores de contingencia se convertirán en servidores de producción y se actualizan los DNS para los usuarios.
- Tendrá un servicio gestionado de respaldos confiable con monitoreo y administración remota.
- Haciendo uso del almacenamiento en nube, se proveerá un servicio que permitirá reducir sus costos de operación y de seguir manteniendo infraestructura tradicional para estas tareas como librerías, cintas y discos.
- La información estará disponible desde cualquier lugar y en cualquier momento.

Gestión del Servicio- Incidentes

- Contacto por Correo o Teléfono
- Asignación de Tickets para seguimiento
- Informe de soporte de incidentes
- Disponibilidad y tiempo de respuesta :

Matriz SLA:

Prioridad	Disponibilidad	Tiempo de respuesta	Descripción
Alta	24 x 7	4 Horas	Incidentes que impactan directamente a la disponibilidad de los servicios relacionados con procesos de negocio críticos del cliente.
Media	8 x 5	12 Horas	Incidentes que no impacta con la disponibilidad del servicio pero que deben ser atendidos en corto plazo ya que esta relacionado con uno o mas procesos de negocio.
Baja	8 x 5	24 Horas	Incidentes que no impactan con la disponibilidad del servicio y que además no están relacionados con procesos de negocio, pero que deben ser atendidos por que podrían ser el inicio de un incidente mayor.

Figura 20. Matriz SLA

Fuente: Recuperado de la política de seguridad de la Fiduciara www.lafiduciaria.com.pe

Organización del Proyecto – Etapas de Implementación

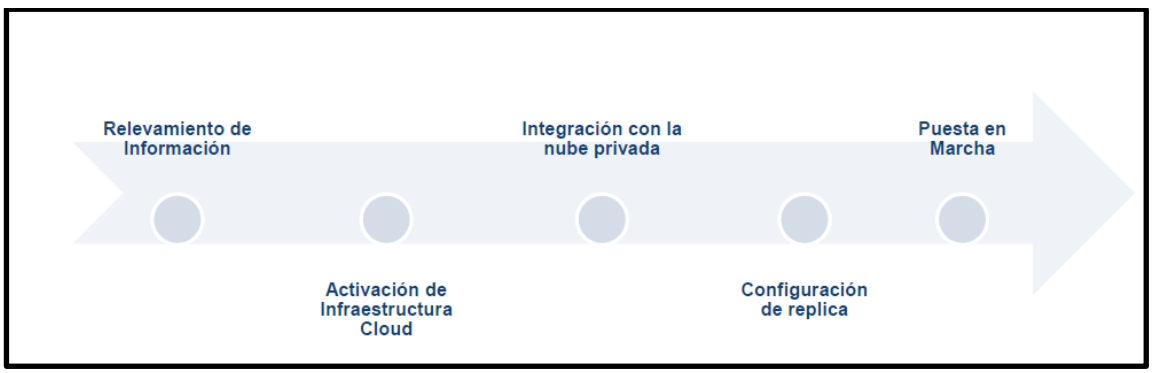


Figura 21. Etapas de Implementación del Proyecto

Fuente: Recuperado de la política de seguridad de la Fiduciaria https://www.lafiduciaria.com.pe

Diagrama de Gantt

WBS	Nombre de tarea	Duration	Start	Finish	% Complete	Resource Names
1	**Implementacion de Continuidad de servicios - LA FIDUCIARIA**	**17 days**	**Mon 26/11/18**	**Mon 17/12/18**	**11%**	**La Fiduciaria**
1.1	**FASE01 - Planificacion - Levantamiento de Informacion**	**1 day**	**Mon 26/11/18**	**Mon 26/11/18**	**100%**	**La Fiduciaria**
1.1.1	Reunion de Kick Off	1 hour	Mon 26/11/18	Mon 26/11/18	100%	La Fiduciaria
1.1.2	Levantamiento de informacion de red - Envio de plantilla	1 hour	Mon 26/11/18	Mon 26/11/18	100%	La Fiduciaria
1.1.3	Definicion de dominio, suscripciones y Licencias para la solucion de continuidad de servicios	1 hour	Mon 26/11/18	Mon 26/11/18	100%	La Fiduciaria
1.1.4	Definicion de Cronograma de actividades	1 hour	Mon 26/11/18	Mon 26/11/18	100%	La Fiduciaria
1.1.5	**HITO: Cronograma de actividades definido**	**1 hour**	**Mon 26/11/18**	**Mon 26/11/18**	**100%**	La Fiduciaria
1.2	**FASE02 - Activacion de Infraestructura**	**4 days**	**Mon 26/11/18**	**Thu 29/11/18**	**17%**	**La Fiduciaria**
1.2.1	Habllitar tenant en Azure para La Fiduciaria	2 hours	Mon 26/11/18	Mon 26/11/18	100%	La Fiduciaria
1.2.2	Habilitar y configurar Suscripcion	3 hours	Mon 26/11/18	Mon 26/11/18	100%	La Fiduciaria
1.2.3	**Configuracion de VPC**	2 days	Tue 27/11/18	Wed 28/11/18	0%	La Fiduciaria
1.2.3.1	Configuracion de red en el Cloud	3 hours	Tue 27/11/18	Tue 27/11/18	0%	La Fiduciaria
1.2.3.2	Configuracion de VPC - Extremo Azure y envio de configuracion al Cliente	1 hour	Tue 27/11/18	Tue 27/11/18	0%	La Fiduciaria
1.2.3.3	Configuracion de firewall de La Fiduciaria	3 hours	Tue 27/11/18	Tue 27/11/18	0%	La Fiduciaria
1.2.3.4	Establecer conexion y pruebas de conexion de Site	2 days	Wed 28/11/18	Thu 29/11/18	0%	La Fiduciaria
1.2.4	**HITO: Infraestructura Activa y conexion establecida con red del Cliente**	**1 hour**	**Thu 29/11/18**	**Thu 29/11/18**	**0%**	La Fiduciaria
1.3	**FASE03 - Despliegue de Infraestructura en nube y Configuracion de replica**	**5 days**	**Wed 17/01/18**	**Tue 23/01/18**	**0%**	**La Fiduciaria**
1.3.1	Despliegue de VMs en Azure	1 hour	Fri 30/11/18	Fri 30/11/18	0%	La Fiduciaria
1.3.2	**Configuracion de DC**	**4 hours**	**Fri 30/11/18**	**Fri 30/11/18**	**0%**	La Fiduciaria
1.3.2.1	Creacion de sites y configuracion de subnets	0.5 hours	Fri 30/11/18	Fri 30/11/18	0%	La Fiduciaria
1.3.2.2	Revision de replicacion de DCs	0.5 hours	Fri 30/11/18	Fri 30/11/18	0%	La Fiduciaria
1.3.2.3	Promover DC de directorio activo en Cloud	2 hours	Fri 30/11/18	Fri 30/11/18	0%	La Fiduciaria
1.3.2.4	Revision de replicacion y validacion de servicio DNS	1 hour	Fri 30/11/18	Fri 30/11/18	0%	La Fiduciaria
1.3.3	**Configuracion de Cloud Backup en File Server**	**16 hours**	**Fri 30/11/18**	**Mon 3/12/18**	**0%**	La Fiduciaria
1.3.3.1	Habilitar storage Account en Azure	0.5 hours	Fri 30/11/18	Fri 30/11/18	0%	La Fiduciaria
1.3.3.2	Definicion de carpetas para copias de seguridad	0.5 hours	Fri 30/11/18	Fri 30/11/18	0%	La Fiduciaria
1.3.3.3	Instalacion de Agente en FS	0.1 hours	Fri 30/11/18	Fri 30/11/18	0%	La Fiduciaria
1.3.3.4	Creacion de tareas de backup	0.2 hours	Fri 30/11/18	Fri 30/11/18	0%	La Fiduciaria
1.3.3.5	Iniciar primera copia de seguridad	9 hours	Fri 30/11/18	Mon 3/12/18	0%	La Fiduciaria
1.3.3.6	Pruebas de restore en FS en Azure	1 hour	Mon 3/12/18	Mon 3/12/18	0%	La Fiduciaria
1.3.3.7	Validacion de permisos NTFS en servidor FS de Azure	3 hours	Mon 3/12/18	Mon 3/12/18	0%	La Fiduciaria
1.3.4	**Configuracion de Mirror SQL Server**	**8 hours**	**Mon 3/12/18**	**Mon 3/12/18**	**0%**	La Fiduciaria
1.3.4.1	Revision de SQL OnPremises	1 hour	Mon 3/12/18	Mon 3/12/18	0%	La Fiduciaria
1.3.4.2	Instalacion de SQL Server	1 hour	Mon 3/12/18	Mon 3/12/18	0%	La Fiduciaria
1.3.4.3	Configuracion de mirror de SQL de dos BD	4 hours	Mon 3/12/18	Mon 3/12/18	0%	La Fiduciaria
1.3.4.4	Validacion de replica de BD en VM en Azure	1 hour	Mon 3/12/18	Mon 3/12/18	0%	La Fiduciaria
1.3.4.5	Configuracion de APP por parte del proveedor de Fiduciaria	2 hours	Mon 3/12/18	Mon 3/12/18	0%	La Fiduciaria
1.3.5	**Replicacion de servidor APP core**	**24 hours**	**Tue 4/12/18**	**Thu 6/12/18**	**0%**	La Fiduciaria
1.3.5.1	Instalacion de agente de Carbonite	1 hour	Tue 4/12/18	Tue 4/12/18	0%	La Fiduciaria
1.3.5.2	Registro de servidores en consola de administracion	1 hour	Tue 4/12/18	Tue 4/12/18	0%	La Fiduciaria
1.3.5.3	Configuracion de replicas	3 hours	Tue 4/12/18	Tue 4/12/18	0%	La Fiduciaria
1.3.5.4	Replicacion de servidor	8 hours	Wed 5/12/18	Wed 5/12/18	0%	La Fiduciaria
1.3.5.5	Validacion de replica de BD en VM en Azure	4 hours	Thu 6/12/18	Thu 6/12/18	0%	La Fiduciaria
1.3.6	**HITO: Sistemas replicados en el Cloud**	**1 hour**	**Thu 6/12/18**	**Thu 6/12/18**	**0%**	La Fiduciaria
1.5	**FASE05 - Pruebas de continuidad**	**1 day**	**Sat 15/12/18**	**Sat 15/12/18**	**0%**	**La Fiduciaria**
1.5.1	Coordinacion de pruebas de continuidad de servicios	1 hour	Sat 15/12/18	Sat 15/12/18	0%	La Fiduciaria
1.5.2	Pruebas de continuidad de servicios	1 hour	Sat 15/12/18	Sat 15/12/18	0%	La Fiduciaria
1.5.3	Retorno de servicios	1 day	Sat 15/12/18	Sat 15/12/18	0%	La Fiduciaria
1.5.11	HITO: Cronograma de actividades definido	**1 hour**	**Sat 15/12/18**	**Sat 15/12/18**	**0%**	La Fiduciaria
1.6	**FASE06 - Puesta de marcha**	**1 day**	**Mon 17/12/18**	**Mon 17/12/18**	**0%**	**La Fiduciaria**
1.6.1	Conformidad de La Fiduciaria	1 hour	Mon 17/12/18	Mon 17/12/18	0%	La Fiduciaria
1.6.2	Presentacion de Informe de cierre de proyecto	1 hour	Mon 17/12/18	Mon 17/12/18	0%	La Fiduciaria
1.6.3	Cierre de Proyecto	1 hour	Mon 17/12/18	Mon 17/12/18	0%	La Fiduciaria

Figura 22. Cronograma del Proyecto
Fuente: Elaboración Propia

Fase 3 Estrategia de Continuidad del Negocio

En esta fase el objetivo de estos planes de continuidad del negocio es recuperar o dar continuidad a la operación de los procesos críticos, dentro de los tiempos objetivos de recuperación definidos. Deben contener como mínimo los siguientes puntos:

- Roles y responsabilidades.
- Criterios de invocación y activación.
- Actividades de preparación, respuesta, operación en continuidad y retorno a la normalidad.
- Información del centro alterno de negocios.
- Requerimiento de recursos.

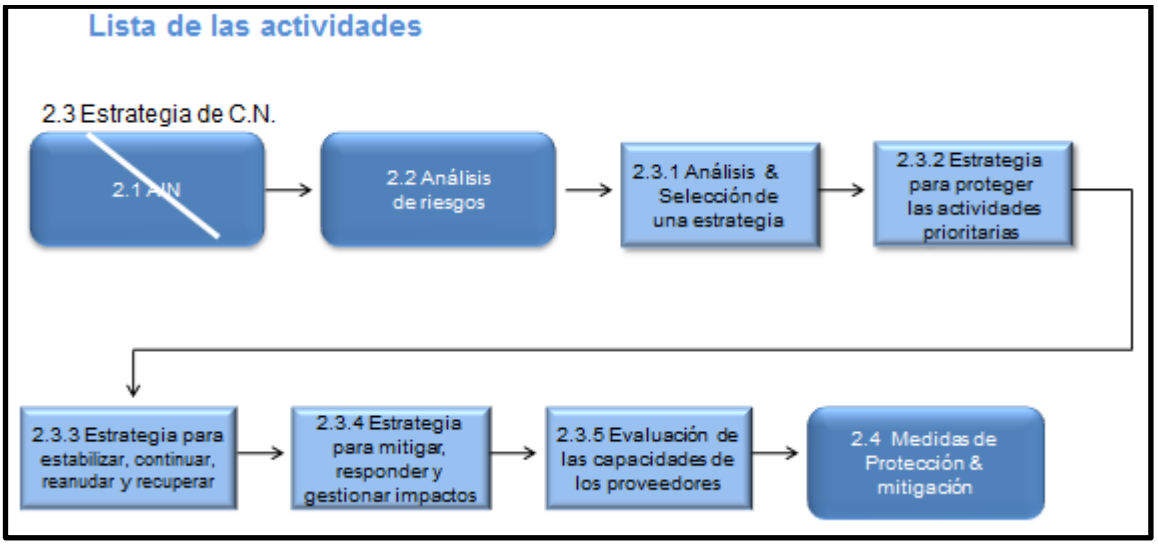


Figura 23. Actividades de Estrategia de continuidad del Negocio

Fuente: Elaboración propia

Análisis y Selección de una estrategia

La empresa cuenta con varios servicios que soportan el giro del negocio, a continuación se indicaran los principales servicios que la empresa necesita para poder realizar sus actividades con normalidad.

Se creará un programa de plan de continuidad para apoyar y garantizar la capacidad de recuperación de las operaciones en condiciones adversas y restaurar los servicios de la empresa en un plazo de tiempo predeterminado y aun nivel aceptable.

Se Incluirá una Política de continuidad del negocio como parte vital en las operaciones y los procesos diarios de la empresa.

Se establecerá y mantener un equipo profesional de gestión de plan de continuidad, para que coordinen las actividades, proporcionar una estructura global y garantizar que las operaciones del negocio se restablezcan.

Identificar los requisitos

Para el desarrollo del proyecto se realizaron reuniones para poder identificar las necesidades alineados a la implementación de un plan de continuidad en el menor tiempo posible con la infraestructura que Microsoft Azure ofrece:

- Backup y recovery a nivel de archivos.
- System otate Backup and bare Metal Recovery.
- Backup de Bases de Datos SQL y Oracle.
- Backup del servidor de correo.
- Almacenamiento en la Nube.
- Backup programado en tiempo real

Responsabilidades específicas:

- Los encargados de adoptar e implementar la continuidad de Infraestructura Tecnológica, también se encarga del Plan de capacitación y concienciación que corresponde a todas las personas que cumplen una función en la gestión de la continuidad.
- Al menos una vez por año deben ser probados y verificados los preparativos relacionados con la continuidad de la Infraestructura Tecnológica, utilizando diversos métodos para evaluar si pueden proteger a las actividades de la organización.
- Los encargados debe redactar un plan de prueba y verificación que debe ser aprobado por la gerencia. Luego de cada prueba y verificación, se debe elaborar un Informe de prueba y verificación.

- Se debe adoptar e implementar el Plan de mantenimiento y revisión del SGCN para que todos los elementos del SGCN estén operativos y actualizados.

- Cuando se activa un Plan de continuidad de Infraestructura Tecnológica, el encargado es el responsable de supervisar la eficacia de la gestión de la continuidad de los sistemas críticos y servicios asociados al negocio.

- Se debe supervisar las no conformidades, falsas alarmas, incidentes reales, etc. y de elevar las acciones preventivas necesarias.

Clasificación de Servicios por Nivel

Funciones de Nivel Primario

Son aquellas funciones que no pueden dejar de operar y que deberán ser repuestas dentro de las siguientes 24 horas de ocurrida la contingencia.

- Podemos considerar dentro de este rango las siguientes:
- Uso de correo electrónico.
- Acceso seguro del Internet.
- Acceso a los sistemas core.

Funciones de Nivel Secundario

Aquí definiremos aquellas funciones que pueden esperar hasta 48 horas antes de convertirse en críticas. Entre ellas tenemos:

- Acceso a documentos del file server.
- Acceso a correos históricos.
- Impresión y emisión de correspondencia, comunicaciones vía teléfono fijo y fax.
- Acceso a correo vía móvil.

Fase 4 Supervisión, medición, análisis y evaluación

En esta fase se va evaluar los impactos de la interrupción de las actividades de la empresa y determinar las prioridades y objetivos de continuidad y recuperación de los servicios.

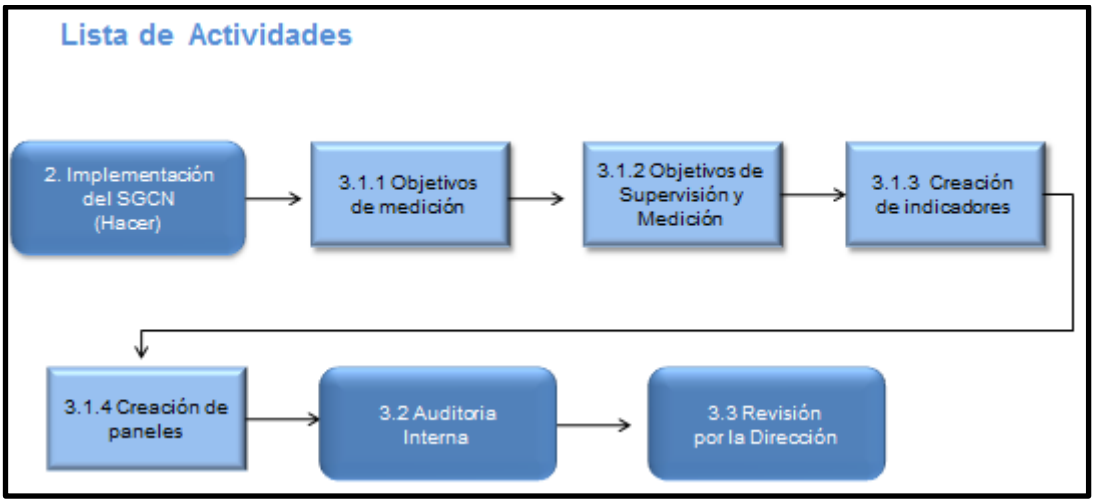


Figura 24. Actividades de Supervisión, Medición, Análisis y Evaluación del SGCN

Fuente: Elaboración Propia

Objetivos de Supervisión y Medición

RPO

El Punto de Recuperación Objetivo o RPO, está íntimamente relacionado hacia la copia de seguridad de datos. Si ocurriese algún tipo de desastre en el centro de datos, la base de datos puede desaparecer o volverse obsoleta e inservible. Como parte del plan de continuidad del negocio, la empresa determino que el tiempo a permitirse en caso de no tener disponible estos datos antes de que falle el negocio, se pierda la reputación, y daño económico.

El tiempo máximo establecido de la última copia de seguridad de los datos de la empresa, respecto a la anterior copia es de 12 horas.

RTO

Es el tiempo objetivo para la reanudación de los servicios después de un desastre.

El tiempo máximo RTO establecido para la empresa es de 4 horas para restauración del aplicativo Gestor, base de datos gestor, acceso a internet, acceso al file server, correos históricos, impresión y emisión de correspondencia.

Análisis de RPO vs RTO

RPO es específicamente el tiempo máximo establecido entre una copia de seguridad y otra con el fin de mantener la continuidad de los servicios. Es esencial para determinar la frecuencia con la que una empresa debe programar copias de seguridad de datos. RTO es el tiempo que tomará una organización para volver a funcionar de acuerdo a los niveles de servicio acordados con sus clientes (sean internos o externos).

Ambos son elementos de recuperación de desastres y de la gestión de la continuidad del negocio.

Auditoria

Los objetivos de la auditoría de la continuidad del negocio son los siguientes:

- Identificar los efectos de las posibles interrupciones de las actividades normales de La Fiduciaria (sean estas resultado de desastres naturales, accidentes, fallas en el equipamiento, acciones deliberadas u otros hechos) y proteger los procesos críticos mediante una combinación de controles preventivos y acciones de recuperación.
- Analizar las consecuencias de la interrupción del servicio y tomar medidas correspondientes de planes.
- Asegurar la coordinación con el personal de la empresa y los contactos externos que participaran en las estrategias de planificación de contingencias. Asignar funciones para cada actividad definida.

Procedimiento de auditoría interna:

Describe todas las actividades relacionadas con la auditoría: redacción del programa de auditoría, selección del auditor, realización de auditorías individuales e informes.

Por otro lado determina si los procedimientos, controles, procesos, acuerdos y demás actividades dentro del SGSN concuerdan con las normas ISO 22301 e ISO 27001, con las regulaciones y documentación interna manejadas por las Empresas Financieras.

El procedimiento se aplica a todas las actividades realizadas dentro del Sistema de Gestión de Continuidad del Negocio (SGCN). Se recomienda realizar al menos 1 auditoría por año y debe cumplir:

- Especificar fechas planificadas y de realización para la auditoría.
- Especificar el alcance de la auditoría áreas, procesos, etc.
- Criterios de auditoría (normas, disposiciones legales, documentación interna)

El impacto en el negocio establece cuantas actividades sostienen a los servicios críticos, de acuerdo a las consultas realizadas se establece los tipos de consecuencias de eventos que detienen los servicios.

Tabla 4.

Eventos de contingencia

Consecuencia insignificante	1	La duración del incidente disruptivo no afecta significativamente las finanzas, las obligaciones legales o contractuales o el prestigio de la organización.
Consecuencia aceptable	2	La duración del incidente disruptivo provoca daños sobre las finanzas, las obligaciones legales o contractuales o el prestigio de la organización, pero ese daño todavía es aceptable teniendo en cuenta su magnitud y circunstancias específicas.
Consecuencia crítica	3	La duración del incidente disruptivo provoca daños sobre las finanzas, las obligaciones legales o contractuales o el prestigio de la organización y ese daño no es aceptable por su magnitud y circunstancias específicas.
Consecuencia catastrófica	4	La duración del incidente disruptivo provoca grandes daños sobre las finanzas, las obligaciones legales o contractuales o el prestigio de la organización que le harán perder la mayor parte de su capital y/o tendrá que cancelar sus operaciones en forma permanente.

Nota. Clasificación de eventos de contingencia. Tomado de la política de seguridad del área de sistemas de la Fiduciaria https://www.lafiduciaria.com.pe

Recolección y Análisis de Información

La recolección y análisis del requerimiento de migración de los sistemas core en la nube para la empresa La Fiduciaria, es proponer una solución con los recursos necesarios que permita poder migrar los servidores core de la empresa a la nube de Microsoft Azure mediante un plan estratégico, para que la operatividad del negocio pueda mantenerse ante cualquier evento que se pueda presentar y así pueda alinearse a las nuevas estrategias y soluciones de TI, mediante la ISO 22301.

Se comprobará que todas las tareas efectuadas en la fase anterior, fueron realizadas de forma correcta, todas las actividades deben garantizar que los servicios se restablecieron satisfactoriamente.

Plan de prueba y verificación:

El objetivo de este Plan es determinar la frecuencia y los métodos de verificación para evaluar la factibilidad de las medidas y de los arreglos para la gestión de la Continuidad del Negocio, como también para establecer las acciones correctivas necesarias.

El Plan contiene un alcance de las pruebas, donde se aplica a todos los elementos que se encuentran dentro del alcance del SGCN, incluyendo los arreglos con los proveedores y socios de la Empresa.

La revisión de los resultados, deben incluir las acciones correctivas correspondientes, como también otras recomendaciones de mejora con su respectivo registro para el control de los resultados.

Fase 5 Mejora Continua

En esta fase se deberá mejorar continuamente la implementación y adecuación del plan de continuidad esto se llevará a cabo con el despliegue del proyecto que a continuación se detalla.

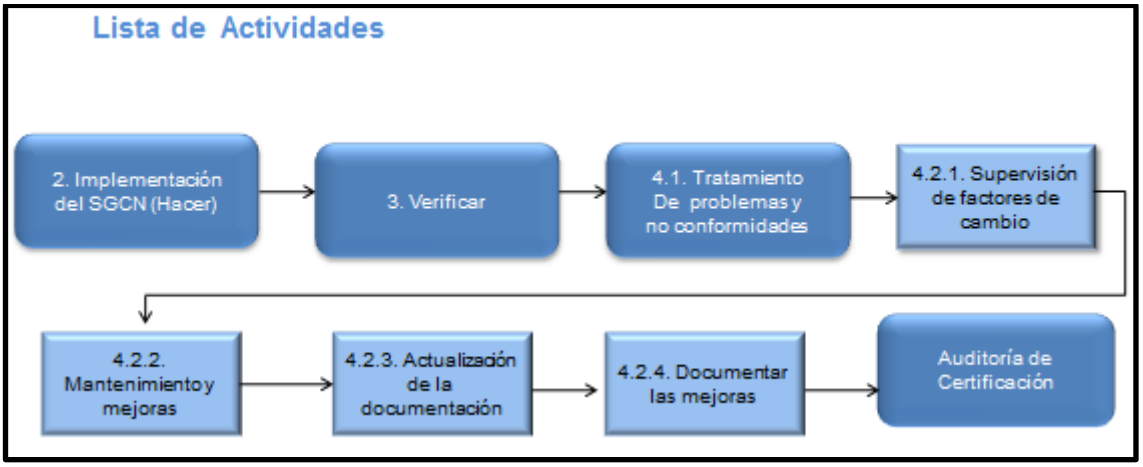


Figura 25. Actividades de Mejora Continua

Fuente: Elaboración Propia

Verificación

Para realizar la integración de la Infraestructura desplegada en la Nube de Azure, es necesario realizar primero la configuración de VPN Site to Site (IPSec) entre la empresa (On-Premises) y Azure. Para ello se muestra el diagrama de conexión VPN a realizar:

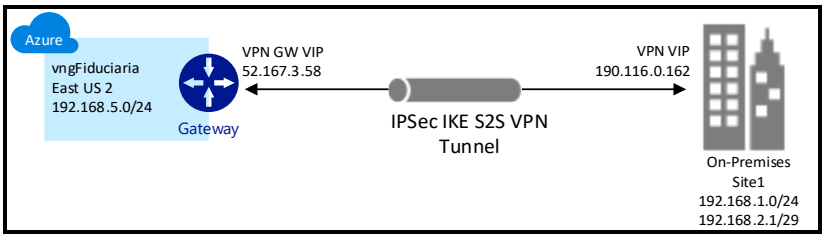


Figura 26. Diseño VPN

Fuente: Recuperado del plan de implementación de Microsoft Azure https://www.azure.microsoft.com

Implementación de Servicios

Se muestra a continuación el proceso de configuración de los diferentes servicios implementados en Azure, para asegurar el plan de continuidad requerido por La Fiduciaria para sus diferentes servicios definidos.

Configuración del Servicio de SQL

Se realizará el aseguramiento del servicio de SQL alojado en el servidor ULISES de la Fiduciaria. Para ello, se procedió a instalar desplegar y configurar un servidor con el servicio de SQL en Azure.

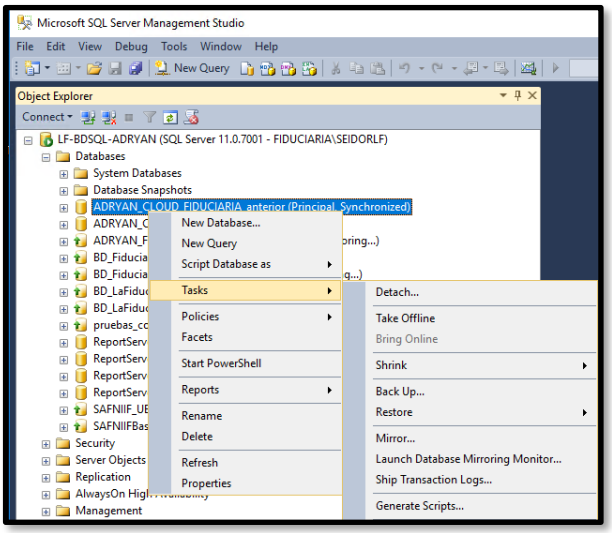


Figura 27. Consola SQL

Fuente: Recuperado de la arquitectura de la base de datos SQL de la Fiduciria.

Configuración del Servicio Carbonite (Servidores Venus – Oracle)

Se realizará la instalación del agente Carbonite en cada servidor (Venus, LF-GESTOR) y se agregar dichos servidores cómo miembros de la réplica.

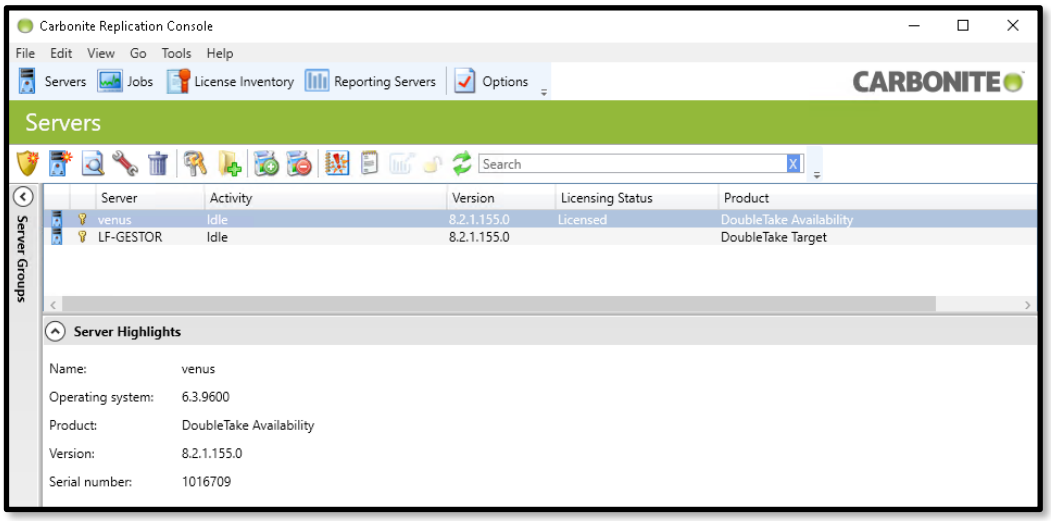


Figura 28. Herramienta Carbonite

Fuente: Recuperado de https://www.carbonite.com

Configuración del Servicio de Cloud Berry

Se realizará la instalación del Agente de la herramienta Cloud Backup en el Servidor Origen (Servidor ATENEO).

La herramienta, se ha configurado para respaldar toda la información en un almacenamiento de Azure de donde se podrá realizar restauraciones periódicas o a necesidad.

Para acceder al aplicativo solo debe ingresar al icono Seidor Cloud Backup, el acceso directo se encuentra en el escritorio del servidor.

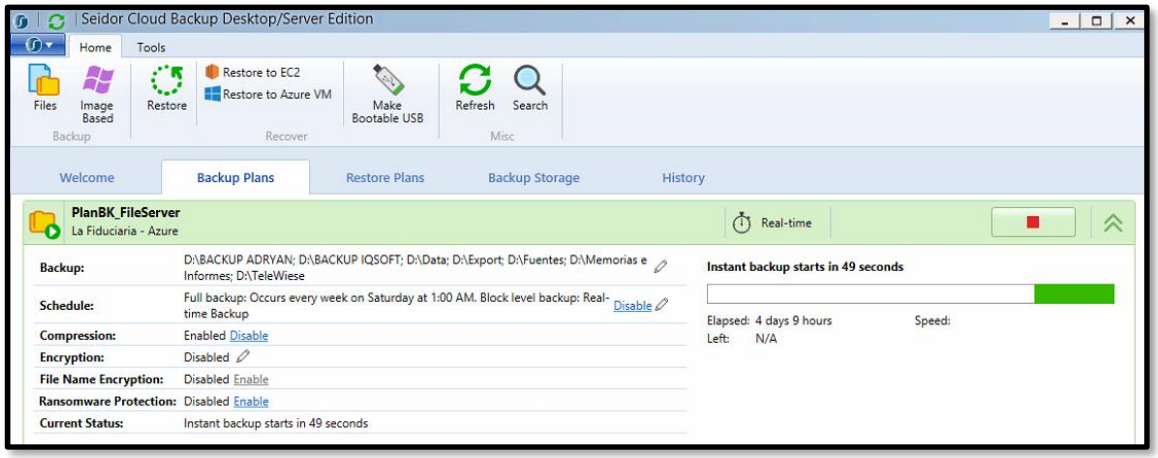


Figura 29. Cloud Backup Seidor

Fuente: Recuperado de https://www.seidor.com

Creación del Job de Respaldo

Se realizará la creación de un job de respaldo que almacenará toda la información de los servidores DataFile.

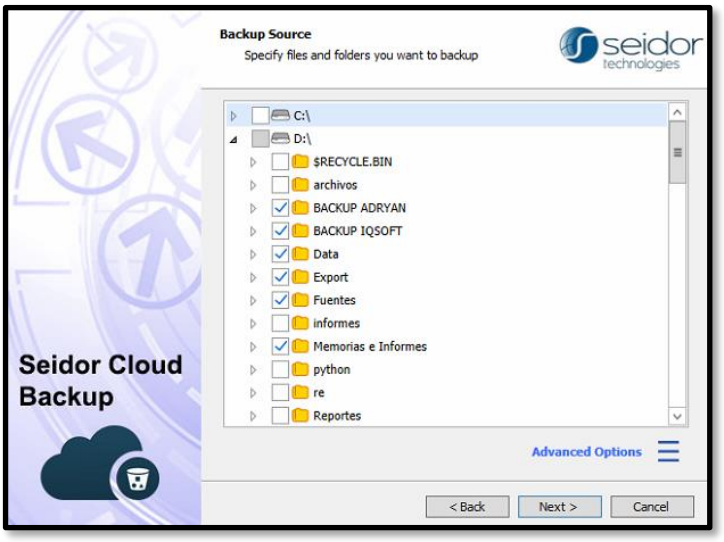


Figura 30. Job de Respaldo

Fuente: Recuperado de https://www.seidor.com

Creación del Job de Restauración

Se realizará pruebas de restauración, para ello se muestra el siguiente procedimiento:
Se ingresará a la herramienta de Cloud Backup, a la sección de Backup Storage. Se busca y define el archivo o carpeta que se desea restaurar:

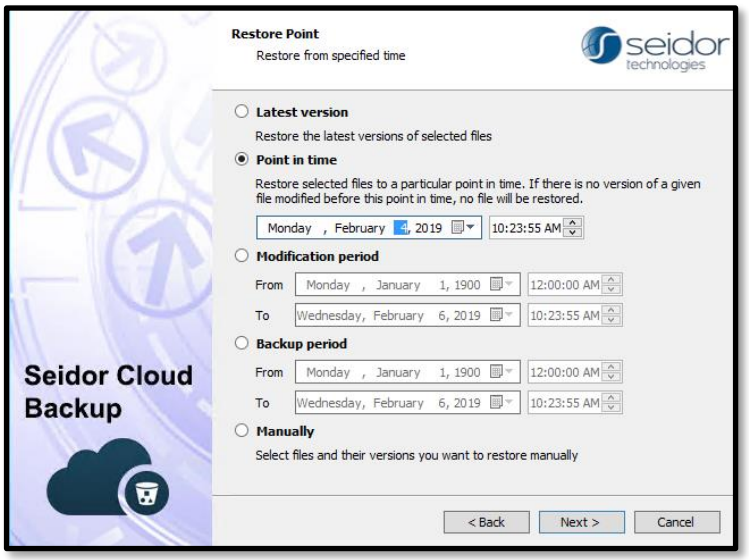


Figura 31. Job de Restauración

Fuente: Recuperado de https://www.seidor.com

Configuración de la Herramienta DFS

Adicionalmente a la aplicación Cloud Backup, se utiliza la herramienta DFS de Windows Server para replicar la información en Línea desde el servidor ATENEO hacia el Servidor de Azure (LF-FS-AZURE) con la finalidad de brindar a La Fiduciaria un escenario de contingencia.

Se instaló la herramienta DFS en ambos servidores, (ATENEO y LF-FS-AZURE) y se realizó la configuración del asistente de replicación:

Desde la consola de DFS, se iniciará un grupo de replicación.

Nos aparecerá un asistente, donde indicaremos el nombre del grupo de replicación:

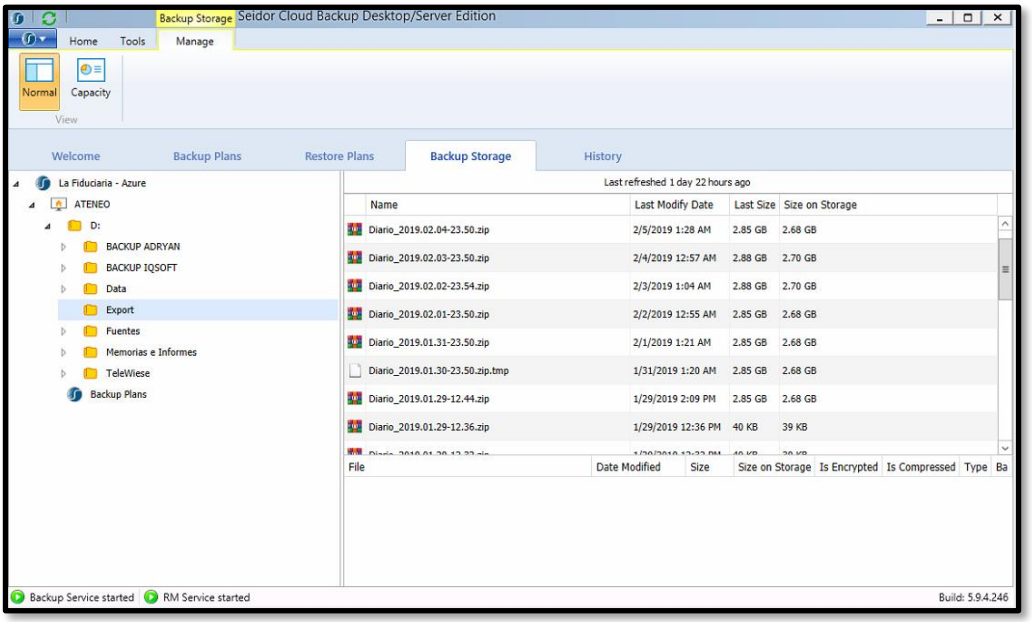


Figura 32. Configuración DFS

Fuente: Recuperado de https://www.seidor.com

Documentar la Mejora

Configuración de VPN Client (Point to Site)

Se realizó la revisión de la configuración del servicio Point to Site de Azure, para permitir la conectividad de los clientes externos (internet) hacia la infraestructura de Azure.

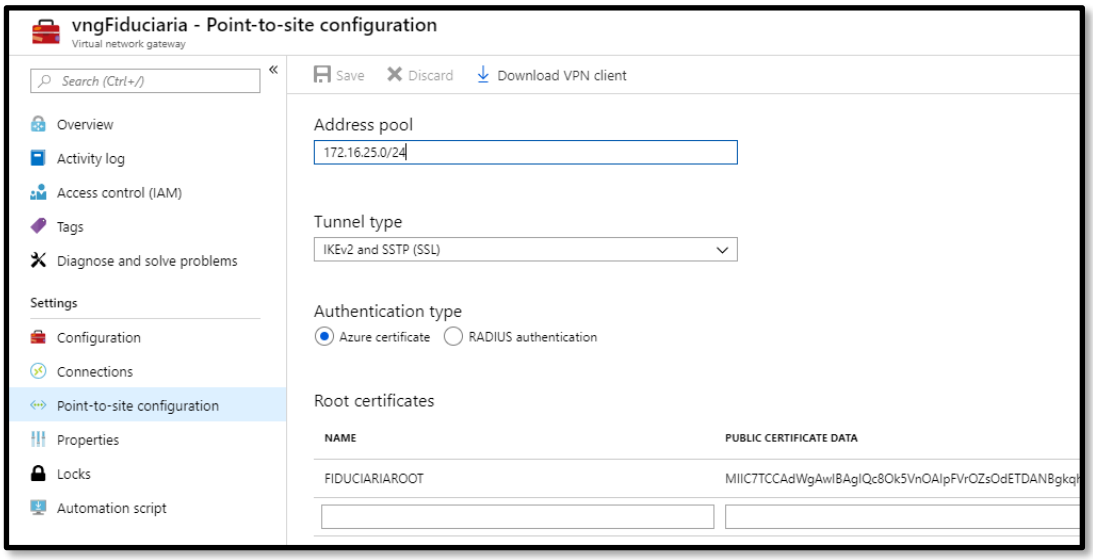


Figura 33. Configuración VPN Point to Site

Fuente: Recuperado de la VPN de la Fiduciaria

Esperar que se complete la instalación y verificarla, ubicando el siguiente ícono:

Desde Network Connections:

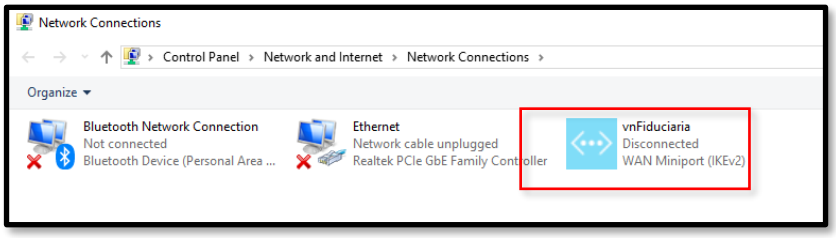


Figura 34. Conexión Disponible

Fuente: Recuperado de la configuración de contingencia de la Fiduciaria

Desde las configuraciones de la PC, en la sección VPN:

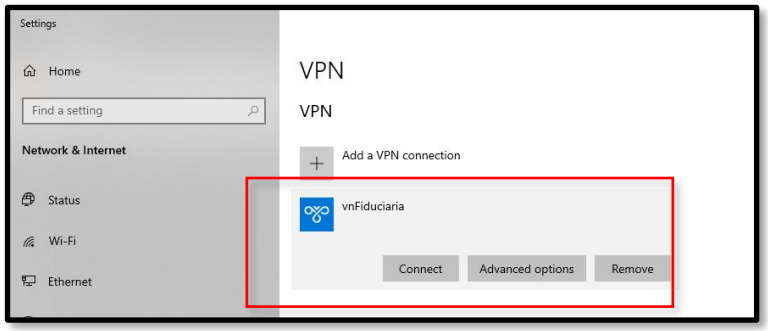


Figura 35. Ejecutar Conexión VPN de contingencia

Fuente: Recuperado de la configuración de contingencia de la Fiduciaria

Validación de Conexión del Cliente VPN

Para conectar el cliente VPN instalado, realizar lo siguiente:

Ingresar a las configuraciones de la PC, en la sección VPN. Ubicar vnFiduciaria, y hacer clic en Connect (Conectar):

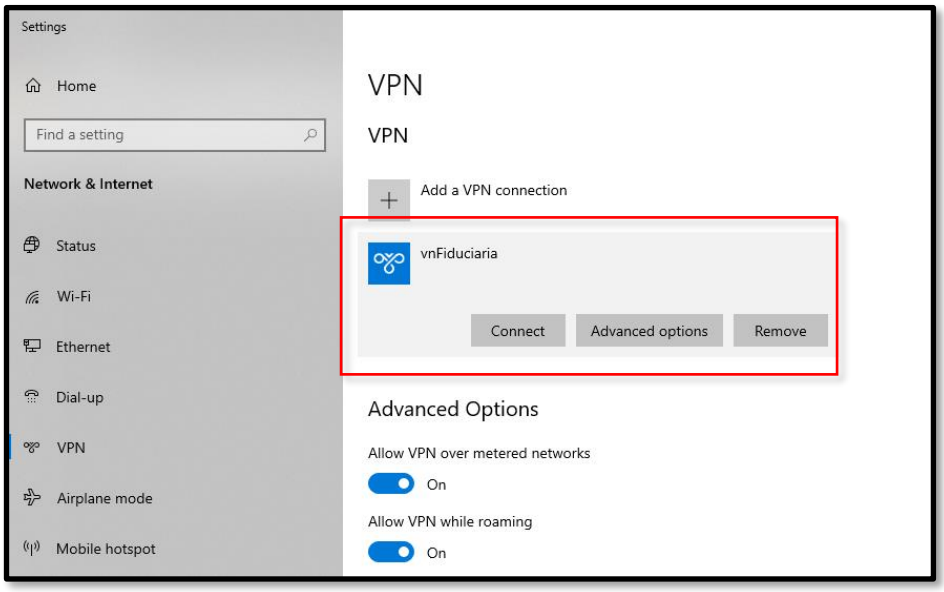


Figura 36. VPN para iniciar la contingencia

Fuente: Recuperado de la configuración de contingencia de la Fiduciaria

Luego, nos aparecerá una ventana Windows Azure Virtual Network. Donde haremos clic en Connect (Conectar):

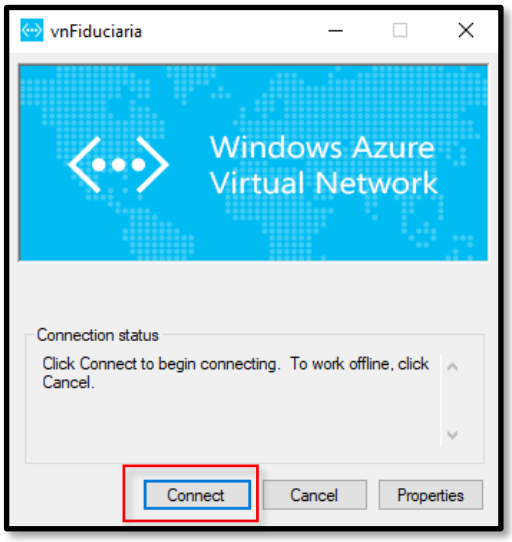


Figura 37. Evento de Conexión

Fuente: Recuperado de la configuración de contingencia de la Fiduciaria

Si aparece un mensaje de confirmación, seleccionar Yes (Si).

Luego validar el estado Connected (Conectado), en la sección de VPN.

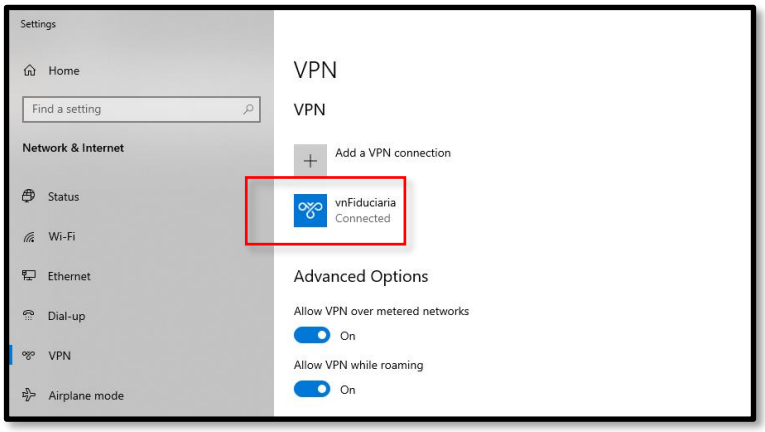


Figura 38. Conexión Establecida

Fuente: Recuperado de la configuración de contingencia de la Fiduciaria

Configuración de la Maquina Cliente

Luego de conectar la Computadora a la VPN de Azure, se deberá realizar lo siguiente para asegurar la conectividad de la PC con los servicios en Azure.

Edición del Archivo Host

Se editará el archivo host por primera y única vez de la máquina cliente. La ubicación del archivo host es la siguiente: C:\Windows\System32\drivers\etc\hosts.

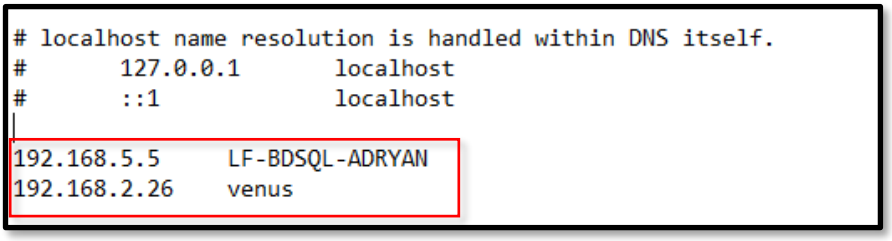


Figura 39. Edición de Archivo Host

Fuente: Recuperado de la configuración de contingencia de la Fiduciaria

Modificación de Script

Se creó un script para el mapeo de carpetas compartidas y la definición de rutas estáticas.

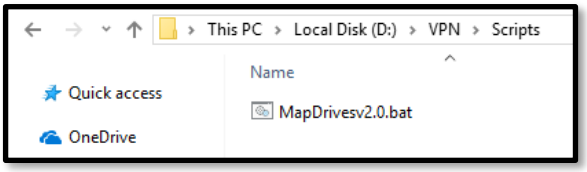


Figura 40. Modificar Script

Fuente: Recuperado de la configuración de contingencia de la Fiduciaria

Luego, se ejecutar el script para configurar el servicio de File Server.

```
net use P: \\192.168.5.7\AdmConta [redacted] /user:fiduciaria\SEIDORLF /persistent:Yes
net use Q: \\192.168.5.7\Archivo_Ft [redacted] /user:fiduciaria\SEIDORLF /persistent:Yes
net use R: "\\192.168.5.7\Cartas DMS" [redacted] /user:fiduciaria\SEIDORLF /persistent:Yes
net use S: "\\192.168.5.7\cartas req. Contable" [redacted] /user:fiduciaria\SEIDORLF /persistent:Yes
net use T: "\\192.168.5.7\Comer Conta" [redacted] /user:fiduciaria\SEIDORLF /persistent:Yes
net use U: \\192.168.5.7\Contabilidad [redacted] /user:fiduciaria\SEIDORLF /persistent:Yes
net use V: \\192.168.5.7\Legal [redacted] /user:fiduciaria\SEIDORLF /persistent:Yes
net use X: \\192.168.5.7\Mkt [redacted] /user:fiduciaria\SEIDORLF /persistent:Yes
net use Y: \\192.168.5.7\Operaciones [redacted] /user:fiduciaria\SEIDORLF /persistent:Yes
```

Figura 41.Ejecutar Script

Fuente: Recuperado de la configuración de contingencia de la Fiduciaria

Verificación de los Servicios de la Empresa

Luego de realizar todas las configuraciones se procederá a validar la conexión de los servicios de La Fiduciaria.

Conexión de Servicio ADRYAN

A través del navegador Internet Explore, se realiza la validación de acceso a la aplicación. Se verificó el acceso correcto a la aplicación Adryan de La Fiduciaria:

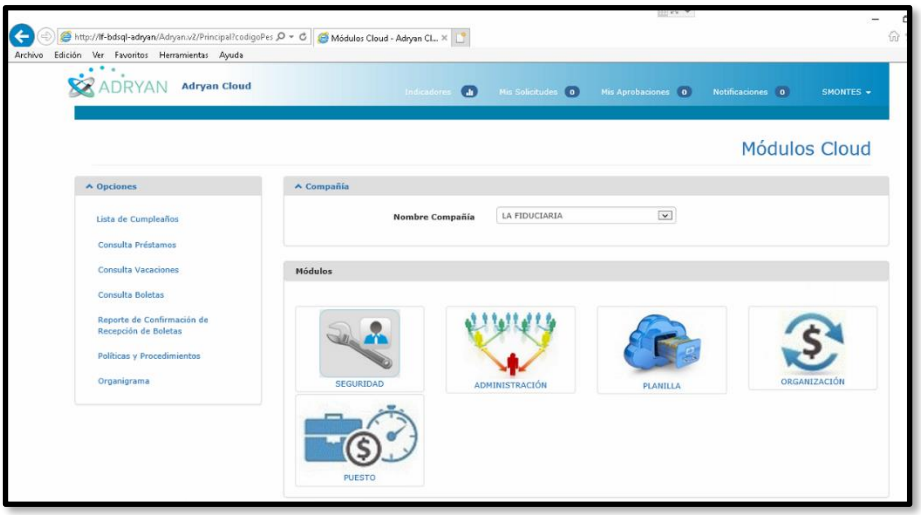


Figura 42. Conexión al Sistema Adryan

Fuente: Recuperado del sistema Adryan de la Fiduciaria

Conexión al Servicio de File Server

A través del explorador de Windows, se realiza la conexión hacia las carpetas compartidas del File Server.

Se verificó el acceso correcto a las carpetas y contenido del servicio de File Server:

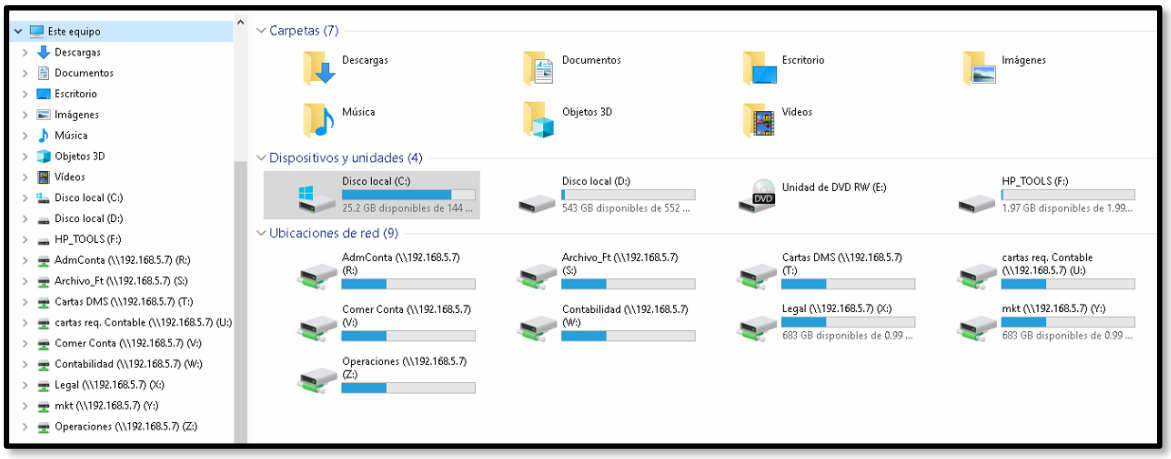


Figura 43. Conexión al File Server

Fuente: Recuperado del data file de la Fiduciaria

Conexión de Servicio Gestor

A través de algún navegador, se realiza la validación de acceso a la aplicación.

Se verificó el acceso correcto a la aplicación Gestor de La Fiduciaria:

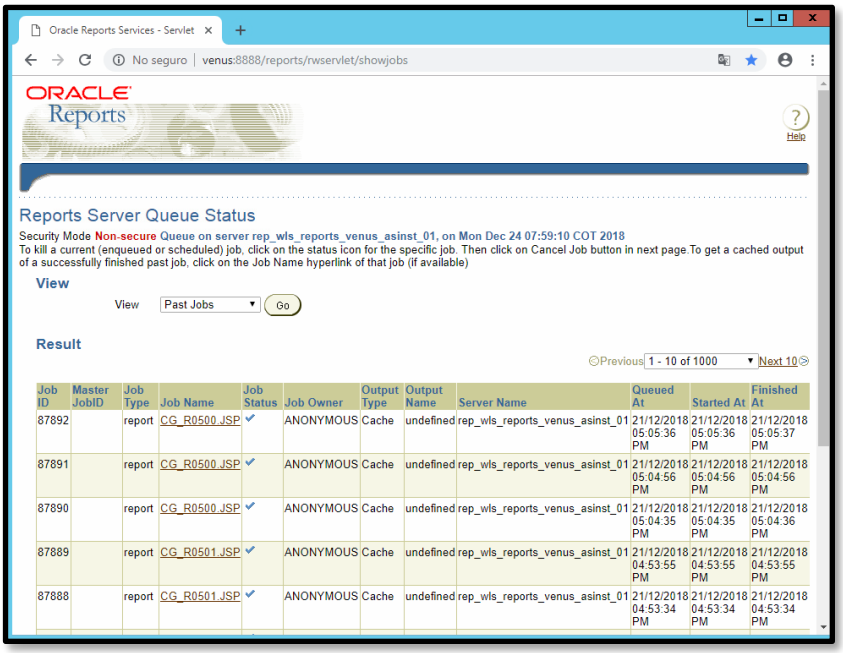


Figura 44. Conexión al Sistema Gestor

Fuente: Recuperado del sistema Gestor de la Fiduciaria

Capítulo V: Análisis y Resultados

Análisis crítico

Según la última Encuesta de Expectativas Macroeconómicas del BCR, las empresas no financieras mantuvieron su proyección de crecimiento para el 2019 en 4,0%. En tanto analistas economías ajustaron a la baja su estimador y esperan una expansión de 3,8%.

Según el BCR, la economía del país habría crecido 4% en todo el 2018, ello con una expansión en el último mes del año superior a 5%.

En tanto, la última Encuesta de Expectativas Macroeconómicas del BCR reportó que el rango de crecimiento económico esperado para 2018 se ubica entre 3.7% y 3.9%

Los analistas económicos esperan una expansión de 3.9% para el 2018, al igual que el sector financiero mientras que las empresas no financieras proyectas un crecimiento de 3.7%.

Resultados

El trabajo en equipo durante esos tres meses dio como resultado la puesta en marcha de los servidores core de la empresa en la nube de Azure basado en los requerimientos de la empresa, se utilizó tecnología de azure y herramientas como el Carbonite y se obtuvo los siguientes resultados

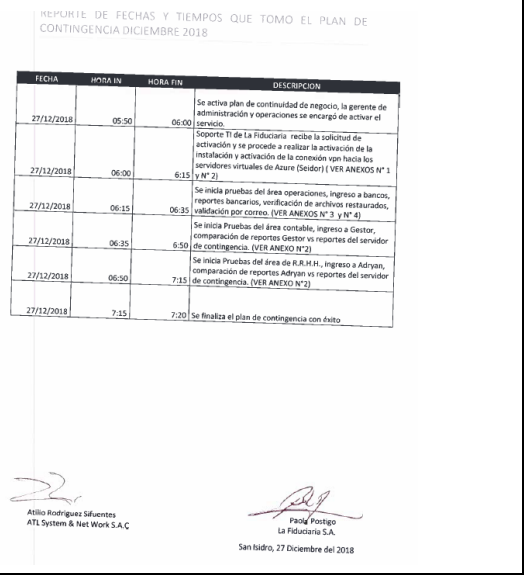
- Cumplimiento de los niveles de disponibilidad acordados.
- Se reducen los costes asociados a un alto nivel de disponibilidad.
- Mayor calidad de servicio.
- Se aumentan progresivamente los niveles de disponibilidad.
- Se reduce el número de incidentes.

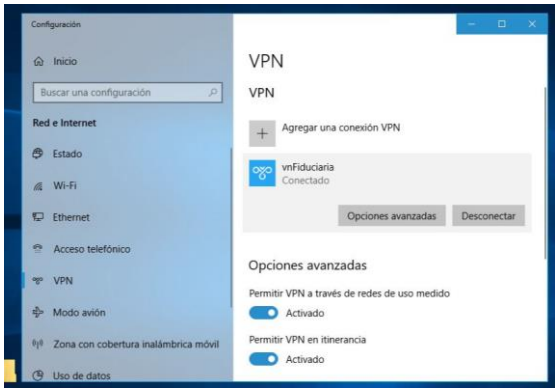
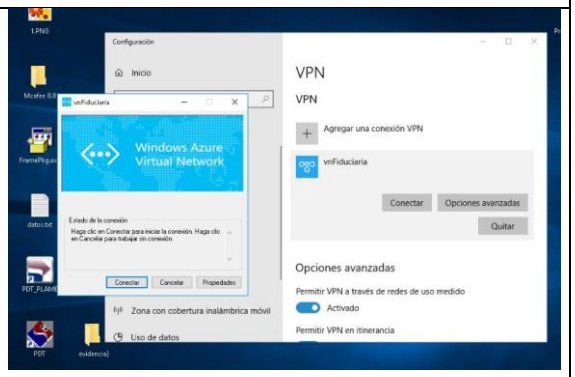
A continuación se muestra un cuadro comparativo de resultados del escenario esperado con el escenario actual

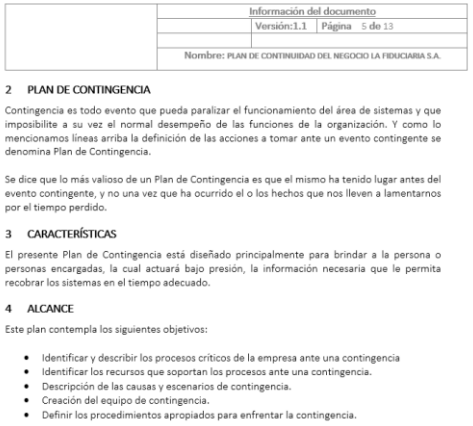
Cuadro comparativo de escenario actual y el escenario esperado de contingencia

Tabla 5.

Cuadro Comparativo de Contingencia

Antes de la Implementación	Después de la Implementación	Evidencia
Los servicios se demoran 48 horas en restablecerse	Los servicios se demoran un máximo de 5 horas en restablecerse	 REPORTE DE FECHAS Y TIEMPOS QUE TOMO EL PLAN DE CONTINGENCIA DICIEMBRE 2018 FECHA / HORA IN / HORA FIN / DESCRIPCION 27/12/2018 05:50 06:00 Se activa plan de continuidad de negocio, la gerente de administración y operaciones se encargó de activar el servicio. 27/12/2018 06:00 6:15 Soporte TI de La Fiduciaria recibe la solicitud de activación y se procede a realizar la activación de la instalación y activación de la conexión vpn hacia los servidores virtuales de Azure (Seidor) (VER ANEXOS N° 1 y N° 2) 27/12/2018 06:15 06:35 Se inicia pruebas del área operaciones, ingreso a bancos, reportes bancarios, verificación de archivos restaurados, validación por correo. (VER ANEXOS N° 3 y N° 4) 27/12/2018 06:35 6:50 Se inicia Pruebas del área contable, ingreso a Gestor, comparación de reportes Gestor vs reportes del servidor de contingencia. (VER ANEXO N°2) 27/12/2018 06:50 7:15 Se inicia Pruebas del área de R.R.H.H., ingreso a Adryan, comparación de reportes Adryan vs reportes del servidor de contingencia. (VER ANEXO N°2) 27/12/2018 7:15 7:20 Se finaliza el plan de contingencia con éxito Atilio Rodriguez Sifuentes ATL System & Net Work S.A.Ç Paola Postigo La Fiduciaria S.A. San Isidro, 27 Diciembre del 2018

Se solicitaba con 24 horas de anticipación un servidor para preparar el plan de contingencia	Se cuenta con servidores en tiempo real en la nube de Microsoft Azure para el plan de contingencia mediante una conexión vpn	
No se cuentan con servidores de producción para el plan de contingencia	Se cuenta con servidores de producción que ante cualquier contingencia se activan en automático	

No se contaba con un plan de contingencia debidamente establecido	Se realizará un plan de contingencia dos veces al años con evidencia de conexión a los servicios	

Nota. Escenarios de Planes de Contingencia. Tomado de la política de seguridad del área de sistemas de la Fiduciaria https://www.lafiduciaria.com.pe

Análisis Económico

La siguiente evaluación económica se realizó teniendo que la mejora del proyecto tiene una vida útil de 3 años y que se realizará de manera pre operativa la migración de servidores a la nube de Microsoft Azure en 3 meses.

Tabla 6.

Datos del proyecto

Datos del Proyecto	Cantidad
Horas al día	**8**
Días al mes	**20**
Consultor TI	***S/. 20.00***
Duración de implementación del proyecto	**3 meses**

Nota. Información del proyecto. Tomado del Excel de cálculo de rentabilidad del proyecto.

Obteniendo los montos por horas relacionados a la mano de obra y el tiempo del proyecto se realizó el siguiente análisis considerando en 3 etapas (3 meses) del proyecto.

Tabla 7.

Salario de personas involucradas en el proyecto por los 3 meses

Descripcion del Puesto	Sueldo Mensual	Sueldo Total (3 meses)
Consultor TI	**S/ 3,200.00**	**S/ 9,600.00**

Nota. Información del proyecto. Tomado del Excel de cálculo de rentabilidad del proyecto

El proyecto se compone de lo siguiente:

Tabla 8.

Descripción y monto de activos y servicios necesarios para el proyecto

Descripción	Importe
LAPTOP	S/ 4,500.00
LICENCIAS	S/ 3,500.00
SERVICIO DE BACKUP	S/ 3,200.00
ESPACIO ADICIONAL	S/ 2,080.80
PERSONAL	S/ 9,600.00
TOTAL PROYECTO	**S/ 22,880.80**

Nota. Información del proyecto. Tomado del Excel de cálculo de rentabilidad del proyecto

Para el cálculo del precio para espacio adicional en la nube se estima que anualmente se incrementará 50GB de almacenamiento en el servidor de Backup.

Tabla 9.

Precio de Gb por mes y año

$/GB*MES	$/GB-AÑO	S/./GB-AÑO	S/./AÑO
0.1	1.2	4.08	693.6

Nota. Información del proyecto. Tomado del Excel de cálculo de rentabilidad del proyecto

El primer año no se consideró espacio adicional, porque el proyecto incluye 1tb de almacenamiento por servidor.

Tabla 10.

Precio por año de GB adicionales

Perio	GB Adicional	Costo	
1 AÑO	0 GB	S/	-
2 AÑO	50 GB	S/	693.60
3 AÑO	100 GB	S/	1,387.20
Total		**S/**	**2,080.80**

Nota. Información del proyecto. Tomado del Excel de cálculo de rentabilidad del proyecto

Al invertir en calidad, toda organización debe tener en cuenta, que el principal objetivo de ello no es principalmente reducir costes.

Uno de los beneficios de invertir en la nube genera es ahorro en no comprar servidores físicos, por lo que no es necesario un espacio, ni contar con centro de datos grandes y amoblados. Solamente paga lo que se utiliza en almacenamiento.

Una vez que se calculó el presupuesto del proyecto, procedemos a obtener el beneficio anual de la inversión al no tener que considerar gastos por operación de servidores físicos

Adicionalmente se conoce que la empresa tiene un COK de 18%.

Tabla 11.

Tabla Resumen para el cálculo de ahorro anual

Ahorro Anual	**SOLES**
Costo de energia de aire acondiconado	S/ 2,551.54
Costo de energia de servidores	S/ 1,453.60
Costo de licencias	S/ 3,400.00
Costo de 10m^2 de oficinas	S/ 6,936.00
Mantenimientos preventivos	S/ 4,080.00
Servicios tecnicos/ mantenimientos reactivos	S/ 1,224.00
Total	**S/ 19,645.14**

Nota. Información del proyecto. Tomado del Excel de cálculo de rentabilidad del proyecto

Tabla 12.

Tabla de Costos para 3 servidores Físicos

Precios	Cantidad		Frecuencia
Costo de mantenimiento preventivo	300	$/mantenimiento	1 mantenimiento cada 3 meses
Costo de incidentes	60	$/incidente	1 incidente cada 2 meses
Licencias	1000	$/anuales	Anual
Precio de espacio de oficina	17	$/m2	mensual

Nota. Información del proyecto. Tomado del Excel de cálculo de rentabilidad del proyecto

Tabla 13.

Tabla de costo por consumo de electricidad

Consumo servidor	188	w
Consumo 3 servidores	564	W
Horas en un mes	720	h
Consumo mensual	406,080	Wh
Consumo mensual	406.08	kWh
Precio kWh	S/ 0.2983	soles/kWh
Coste mensual	S/ 121.13	soles
Coste anual	**S/ 1,453.60**	soles
Consumo aire acondicionado	0.99	kWh
Horas en un mes	720	h
Consumo mensual	712.8	kWh
Precio kWh	S/ 0.2983	soles/kWh
Coste mensual	S/ 212.63	soles
Coste anual	**S/ 2,551.54**	soles

Nota. Información del proyecto. Tomado del Excel de cálculo de rentabilidad del proyecto

Tabla 14.

Tabla de cálculo de depreciación y amortización del proyecto

Descripción	Importe	Vida util años	Depreciación anual	Amortización anual	Valor en Libros al tercer año
LAPTOP	S/ 4,500.00	4	1,125.00		1,125.00
LICENCIAS	S/ 3,500.00	3		1,166.67	-
SERVICIO DE BACKUP	S/ 3,200.00	3		1,066.67	-
ESPACIO ADICIONAL	S/ 2,080.80	3		693.60	-
PERSONAL	S/ 9,600.00				
TOTAL PROYECTO	**S/ 22,880.80**			**2,926.93**	

Nota. Información del proyecto. Tomado del Excel de cálculo de rentabilidad del proyecto

Al final de los 3 años del proyecto, el único activo que tendrá valor en libros es la laptop. Y se venderá con un valor de mercado de S/. 1,000.00 soles.

Con la información analizada se va a realizar el siguiente flujo de trabajo.

Tabla 15.

Tabla de flujo neto de fondos económicos

AÑO	AÑO 0	AÑO 1	AÑO 2	AÑO 3
BENEFICIOS		**S/ 19,645.14**	**S/ 19,645.14**	**S/ 19,645.14**
(-)DEPRECIACION		S/ 1,125.00	S/ 1,125.00	S/ 1,125.00
(-)AMORTIZACION		S/ 2,926.93	S/ 2,926.93	S/ 2,926.93
VALOR DE MERCADO				S/ 1,000.00
(-)VALOR EN LIBROS				S/ 1,125.00
UTILIDAD ANTES DE IMPUESTOS		**S/ 15,593.21**	**S/ 15,593.21**	**S/ 15,468.21**
(-)IMPUESTO (28%)		S/ 4,366.10	S/ 4,366.10	S/ 4,331.10
UTILIDAD DESPUES DE IMPUESTOS		**S/ 11,227.11**	**S/ 11,227.11**	**S/ 11,137.11**
DEPRECIACION		S/ 1,125.00	S/ 1,125.00	S/ 1,125.00
AMORTIZACION		S/ 2,926.93	S/ 2,926.93	S/ 2,926.93
VALOR EN LIBROS		S/ -	S/ -	S/ 1,125.00
(-)INVERSION TOTAL	-S/ 22,880.80			
FNFE	**-S/ 22,880.80**	**S/ 15,279.04**	**S/ 15,279.04**	**S/ 16,314.04**

Tabla 16.

Tabla de periodo de recuperación de Inversión

	AÑO 0	AÑO 1	AÑO 2	AÑO 3
FNFE	-S/ 22,880.80	S/ 15,279.04	S/ 15,279.04	S/ 16,314.04
DESCONTADOS	-S/22,880.80	S/12,948.34	S/10,973.17	S/9,929.23
ACUMULADOS	-S/22,880.80	-S/9,932.46	S/1,040.71	S/10,969.95

Nota. Información del proyecto. Tomado del Excel de cálculo de rentabilidad del proyecto

Tabla 17.

Tabla de cálculo de periodo de recuperación de inversión

RECUPERACIÓN DE INVERSIÓN	1.90 años
AÑOS	1
MESES	10
DIAS	23

Nota. Información del proyecto. Tomado del Excel de cálculo de rentabilidad del proyecto

Según la tabla anterior, en el flujo neto de fondos económicos se puede observar que el periodo de recupero del proyecto es 1 año, 10 meses y 23 días.

Tabla 18.

Tabla del cálculo del VAN, TIR, ROI y beneficio costo

VAN ECONOMICO	**10,969.95**
B/C ECONOMICO	**1.48**
TIR	**45.98%**
ROI	**47.94%**

Nota. Información del proyecto. Tomado del Excel de cálculo de rentabilidad del proyecto

Con este cálculo se deduce que el proyecto de inversión es rentable.

Conclusiones

Como resultado de este trabajo se ha concluido en lo siguiente:

1. Al tener como resultado una TIR (Tasa Interna de Retorno) de 45.9%, y un COK (Costo de Oportunidad de Capital) proporcionado por la empresa de 18%, se concluye que el proyecto es una alternativa atractiva para la empresa al ser el retorno mayor al mínimo aceptable.
2. Se logró implementar los servidores en la nube de Azure reduciendo el tiempo de reanudación de los servicios a un 33% a comparación con la situación anterior.

3. Se implementó una política y procedimiento del plan de continuidad de la empresa. Para que pueda ser divulgado con todos los colaboradores de la empresa

4. Se implementaron servidores virtuales para que realice la replicación de la información en tiempo real.

5. La Fiduciaria como parte del Plan de Continuidad del negocio se ha considerado un análisis del impacto financiero el cual permitirá estimar las pérdidas financieras por incapacidad para atender las obligaciones contractuales de cada fideicomiso así como daños al personal.

6. La Fiduciaria considera un promedio de monto de pérdidas diarias por concepto de cuotas no atendidas de 8,687.22 soles y 17,276.51 dólares, si bien económicamente La Fiduciaria puede solventar esos gastos por un periodo mayor, se presume que se perdería la confianza de los clientes en un periodo de 15 días momento en el cual la empresa podría dejar de operar.

7. Para efectos del presente y con el nuevo proyecto de continuidad del negocio el monto de las perdidas será revisadas cada año.

8. Se espera que con la inversión del proyecto genere un margen menor de pérdidas ante una contingencia.

Recomendaciones

Como resultado de este trabajo se plantea las recomendaciones siguientes:

1. Elegir un proveedor cloud que pueda demostrar la validación de los controles que utiliza en cuanto a datos, accesibilidad, seguridad del centro de datos, encriptación de la información y certificación SSAE 16.

2. Optar por una nube privada, o por una nube privada virtual, donde los sistemas son virtualmente separados entre sí a través de un entorno encriptado dentro de una nube pública.

3. Analizar qué aplicaciones de las ya existentes son más apropiadas para la nube.

4. Exigir el envío de alertas de eventos de seguridad especialmente sobre activos de misión crítica.

5. Realizar auditorías externas a la empresa para conseguir una mayor transparencia y comprobar el cumplimiento de las certificaciones clave de la industria como ISO 27001 y 27002, ISO 31000.

6. Añadir medidas de seguridad adicionales como acceso de firma única (single sign-on) a múltiples aplicaciones en la nube y emplear además marcos de seguridad como ITIL o ITSM.

Referencias

López Trujillo, Marcelo, et al. "Servidos de gestion de conocimiento utilizando la computacion en nube." Entre Ciencia e Ingeniería, vol. 5, no. 9, 2011, p. 170+. Gale OneFile: Informe Académico, https://link.gale.com/apps/doc/A312828709/GPS?u=usil&sid=GPS&xid=5cb21893. Accessed 21 Sept. 2019.

Arana López, Liz Melissa, et al. "Análisis de aplicaciones empleando la computacion en la nube de tipo PaaS y la metodología ágil Scrum." *Industrial data*, vol. 18, no. 1, 2015, p. 149+. *Gale OneFile: Informe Académico*, https://link.gale.com/apps/doc/A597962040/GPS?u=usil&sid=GPS&xid=d0289819. Accessed 21 Sept. 2019.

Varela Pérez, Carlos Fernando, et al. "COMPUTACION EN LA NUBE: UN NUEVO PARADIGMA EN LAS TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACION." *Redes de Ingeniería*, vol. 8, 2017, p. 138+. *Gale OneFile: Informe Académico*, https://link.gale.com/apps/doc/A568973241/GPS?u=usil&sid=GPS&xid=e5547095. Accessed 21 Sept. 2019

Duch, L. (2016, Aug 10). Las empresas frente a las amenazas externas. Cinco Dias Retrieved from https://search.proquest.com/docview/1810468736?accountid=43847

Planas, M. (2015, Aug 17). ¿Necesitas un plan de continuidad de negocio? Cinco Dias Retrieved from https://search.proquest.com/docview/1704416406?accountid=43847

Mircrosoft Azure . (2019). *Productos Azure*. Obtenido de Sitio Web Microsoft Azure: https:// https://www.azure.microsoft.com/es-es/services/

La Fiduciaria . (2019). *Productos y Servicios del fideicomiso* . Obtenido de Sitio Web La Fiduciaria : https:// https://lwww.afiduciaria.com.pe

EY (2018). *La Ciberseguridad es algo mas que protección?*. Obtenido de Sitio Web de EY : https://www.ey.com/Publication/vwLUAssets/ey-encuesta-global-seguridad-informacion-2018-19/.pdf.

Luz del sur. (2019). Precios para venta de energía electrica Obtenido de Sitio Web de Luz del sur : https://www.luzdelsur.com.pe/media/pdf/tarifas/TARIFAS.pdf.