



**DECANATO DE INGENIERÍA E INFORMÁTICA**

**“PROPUESTA DE TRABAJO DE GRADO”**

**“EVALUACIÓN DE RIESGOS Y CONTROLES PARA EL USO DE TECNOLOGÍA CLOUD**

**HÍBRIDA EN GSI INTERNATIONAL”**

Propuesta de la monografía para optar por el título de:

**INGENIERÍA EN SISTEMAS DE INFORMACIÓN**

**SUSTENTANTES:**

MARIA TERESA CIRIACO  
ELISEO SANTANA  
EDGAR PAYANO

2008-1736  
2011-1552  
2012-2445

**ASESORES:**

NIURKA HERNANDEZ  
WILLY PADUA

Santo Domingo, D.N.

Abril 2020

**“EVALUACIÓN DE RIESGOS Y CONTROLES PARA EL USO DE TECNOLOGÍA  
CLOUD HÍBRIDA EN GSI INTERNATIONAL EN LA CIUDAD DE SANTO DOMINGO.  
REPÚBLICA DOMINICANA. AÑO 2020.”**

## INDICE

AGRADECIMIENTOS .....	5
DEDICATORIAS.....	9
RESUMEN.....	12
INTRODUCCIÓN.....	12
CAPÍTULO I. ASPECTOS GENERALES .....	15
1.1 Marco Legal.....	15
1.2 Concepto.....	17
1.2 Historia .....	18
Conclusión. ....	21
CAPÍTULO II. TECNOLOGÍA CLOUD.....	23
Introducción.....	23
2.1 Conceptos Cloud.....	23
2.2 Clasificación y características .....	23
2.3 Requerimientos .....	25
2.4 Ventajas y desventajas .....	26
2.4.1 Desventajas Tecnología Cloud Híbrida .....	27
Conclusión. ....	27
CAPÍTULO III. EVALUACIÓN Y GESTIÓN DEL RIESGO TECNOLÓGICO.....	29
Introducción.....	29
3.1 Conceptos .....	29
3.1.1 Definición Evaluación.....	29
3.1.2 Riesgo.....	29
3.1.3 Riesgo Tecnológico.....	29
3.1.4 Evaluación de Riesgo Tecnológico .....	30
3.1.5 Controles.....	31
3.1.6 Amenaza.....	31
3.1.7 Seguridad.....	31
3.1.8 Riesgo tecnológico orientado a servicios Cloud.....	31
3.1.9 Herramientas para seguridad.....	32
3.1.10 Integración con otros servicios.....	32

Conclusión .....	34
CAPÍTULO IV. HERRAMIENTAS Y SOLUCIONES PARA NEGOCIOS .....	36
Introducción.....	36
4.1 Conceptos de las Herramientas .....	36
Conclusión .....	38
CAPÍTULO V. SISTEMA .....	39
Introducción.....	39
5.1 Software .....	39
5.2 Base de Datos.....	39
5.3 Servidores .....	40
Conclusión .....	40
CAPÍTULO VI. METODOLOGÍA.....	42
Introducción.....	42
Metodología .....	42
6.1 Tipos de investigación.....	42
6.2 Métodos .....	43
6.3 Población y Muestra.....	45
6.4 Técnicas e Instrumentos .....	46
Uso de Controles de redes sólidos .....	51
Alta disponibilidad .....	51
Protección contra DDoS.....	52
Escalabilidad de carga .....	52
CONCLUSIÓN Y RECOMENDACIONES .....	58
BIBLIOGRAFÍA.....	62
ANEXOS .....	64
ANEXO I - Anteproyecto .....	64
ANEXO II- Modelo de Cuestionario para implementación de verticales .....	82

## **AGRADECIMIENTOS**

### **A mi madre**

María Lidia, gracias por tu dedicación, amor y entrega constante, por tus consejos y enseñanzas, sin tu ejemplo de superación no estaría aquí en este momento culminando esta etapa de mi vida.

### **A mis hermanas**

Ángela María y Crystal, gracias por siempre apoyarme en mis decisiones, por sus consejos y por todo su amor.

### **A mis suegros**

Iris Heyaime y Antonio Tueni, gracias por todo su amor, entrega y apoyo en todos los sentidos durante esta etapa de mi vida.

### **A mis compañeros y Profesores**

A todos aquellos que de alguna manera aportaron durante mi carrera en la universidad, en especial a mis compañeros de área Eliseo y Edgar que hicieron posible esta entrega de monografía. Gracias de corazón a todo el equipo de profesores, por todo su apoyo y seguimiento principalmente los de mi área de tecnología y a mis asesores de monografía Niurka Hernández y Willy Padua.

Por último y el más importante, gracias a ti mi DIOS porque hiciste que todo esto fuera posible.

**María Teresa Ciriaco**

## AGRADECIMIENTOS

En primer lugar, quiero agradecer a Dios y a toda mi familia, Mi madre Mercedes Hernández que siempre me dio ánimos y me incitaba para que siguiera adelante, mi padre Domingo Santana que siempre me brindó su apoyo incondicional y me ha dado siempre los mejores consejos, no solo para la universidad sino consejos de vida.

A mis hermanos Rafael Santana, Kelvin Santana y Keidy Santana, quienes de una manera u otra me apoyaron en todo momento, a veces hasta de forma económica, a mi Gemelo Greidy Santana que siempre ha estado conmigo y de hecho hemos tomado materias juntos, hemos crecido juntos y bueno lo esperare en la meta hasta que también termine este largo caminar, a mi hermana Gisell que siempre me dio fuerzas y me ayudaba en todo lo que podía, dándole ese toque de elegancia a algunos de mis trabajos.

En otro orden, quiero agradecer a mis compañeros de monográfico, Maria Ciriaco y Edgar Payano, quienes me han apoyado de una manera especial, nos conocemos desde cursos anteriores y ha sido para mí todo un placer conocer y compartir con personas tan excepcionales.

Sé que es imposible agregar a todas las personas que me apoyaron y que ayudaron que este sueño sea posible, pero mencionare a las personas que fueron más influyentes, Eliezer de León mi hermano y amigo que iniciamos la universidad juntos y pasamos muchas cosas juntas, muchas altas y bajas, Ana Satiel, creo que no tengo palabras para agradecer todo lo que ella ha hecho por mí en estos años de carrera, pero aun así intentaré resumirlo en pocas palabras: fue mi compañera y mentora.

Mis amigos Sarelvis Guillen, Jason de Jesús, Jhiira Girón, entre otros, que hicieron mi proceso en UNAPEC mucho más llevaderos, divertidos y que me demostraron que esta generación de profesionales que se aproxima seremos los mejores en mucho tiempo.

En último lugar, pero no menos importante quiero agradecer de una manera súper especial a mi segunda madre Evelyn Carvajal (Kerna), ella siempre me instó a nunca

rendirme, a soñar en grande, me dijo que por más difícil que fuera trabajar y estudiar el mismo tiempo, ella confía que lo lograré, de alguna manera fue su apoyo y su confianza en mí lo que me ayudó a no rendirme en determinados momentos

**Eliseo Santana**

## **AGRADECIMIENTOS**

Primero agradecer a Dios, por permitirme culminar esta etapa de mi vida, este logro que ha sido bastante retador, pero he salido airoso y ya pasare a ser un profesional, un logro del cual debe sentirse orgulloso todo el que lo consigue.

En este orden, agradecer a mi familia, mi madre Sonia Carrasco, mi padre Edgar B. Payano, mi hermana Lined Payano, que siempre han estado dispuestos a ayudarme en todo lo que he necesitado, desde tareas sencillas hasta cualquier consejo para desarrollar cualquier actividad. Gratitud especial para mi madre, que siempre se mantuvo a la espera de la culminación de mi etapa universitaria con mucha paciencia, también a mi padre.

Mis agradecimientos continúan con todas aquellas personas que de una manera u otra aportaron de manera positiva a mi carrera, amigos que me ayudaron con muchas explicaciones en asignaturas que no dominaba por completo, gracias a ellos pude continuar de manera exitosa con mi carrera.

Están mis compañeros de Monográfico: María Ciriaco y Eliseo Santana, quienes tomaron otras asignaturas conmigo durante la carrera y siempre estuvieron dispuestos a ayudar de cualquier manera posible, siempre apoyándonos y ayudándonos con todo este proceso, que sabemos que no es nada fácil, gracias por todo.

Por último, pero no menos importante a toda mi familia, que siempre está presente cuando los necesito, agradecido eternamente de todo aquel que de manera directa o indirecta contribuyo con mi carrera que, con mucho esfuerzo y sacrificios, culmina de manera exitosa.

¡Ya somos Ingenieros!

**Edgar Payano**

## **DEDICATORIAS**

### **A mi Esposo e Hijas,**

José Miguel Tueni, Iris Sofía y Victoria Maria que son la razón de todo mi esfuerzo y dedicación, representan todo mi amor y felicidad. Sin ustedes este sueño no sería posible, muchas gracias por estar conmigo.

**María Teresa Ciriaco**

## **DEDICATORIAS**

Esta monografía la dedico a mis padres Domingo Santana y Mercedes del Carmen Hernández, quienes me apoyaron en todo momento, entiendo que sin ellos este camino hubiese sido más difícil.

**Eliseo Santana**

## **DEDICATORIAS**

A mi familia, a todos ellos en general, por el apoyo brindado a lo largo de mi carrera, inmensamente agradecido.

**Edgar Payano**

## **RESUMEN**

Este proyecto presenta una investigación sobre la evaluación y gestión de riesgo para uso de tecnología cloud de la empresa SGI International en la ciudad de Santo Domingo.

A su vez incluye todo lo que compone un sistema implementado de manera correcta en una tecnología cloud a nivel de seguridad, infraestructura acoplado el marco legal, protocolos de comunicación, características, modelos de estructuras, servidores y bases de datos, así como interfaces de usuario para entrada y salida.

## **INTRODUCCIÓN**

A partir de esta investigación se busca evaluar los riesgos y a la vez, establecer controles al momento de adquirir la tecnología cloud híbrida para la empresa GSI International, lo que se debe tomar en cuenta y lo que se debe hacer para llevar a cabo la migración de información hacia la nube, como manejar todo con el debido nivel de seguridad para mantener la integridad de los datos importantes de la antes mencionada empresa. De esta manera también se busca mejorar la inversión económica en la empresa, ya que la implementación de dicha tecnología tiende a mejorar todo lo que tiene que ver con los procesos en la empresa y aunque esto conlleva un precio, la relación beneficio-costos es mucho mejor que al no tenerla.

Esta investigación es conveniente porque a partir de ella se puede determinar una propuesta acertada a la empresa GSI International para fines de la evaluación y gestión del riesgo tomando en cuenta la migración de procesos hacia una tecnología cloud híbrida, este paso traería consigo mayor posicionamiento a nivel de mercado y la expansión de la cartera de clientes.

Este tipo de tecnología tiene como objetivo simplificar y brindar opciones adicionales a pequeñas y medianas empresas del sector bancario para poder obtener servicios en las nubes de procesos automatizados y/o adaptados a su empresa con un menor costo, esto debido a que requeriría menos inversión de tiempo y de personal para desarrollo.

En la actualidad existen diferentes empresas internacionales de renombre que ofrecen este tipo de servicios y entre las principales ventajas que se encuentran en la tecnología cloud híbrida está el acceso desde cualquier dispositivo, actualización constante de tecnología, pago por el uso de servicio de acuerdo a lo establecido, capacidad de almacenamiento ilimitada, disminución de uso de hardware, entre otros.

Otros de los beneficios que brinda esta tecnología es el servicio confiable, flexible y de alta escalabilidad.

La prioridad de desarrollar este tema es mejorar el catálogo de productos a ofrecer a los clientes y con esto poder brindar un mejor servicio mediante la aplicación de la tecnología Cloud Híbrida, esto produciría una mejora en el trabajo diario de cada uno de sus clientes, además se estaría posicionando a dicha empresa en un rango mayor ya

que es importante mantenerse innovando y buscando mejores formas de hacer las cosas, tratando siempre de usar e implementar las últimas tecnologías disponibles.

Objetivo general:

Evaluar los riesgos y controles para el uso de tecnología Cloud Híbrida en GSI International.

Objetivos específicos:

Objetivo 1:

Analizar los requerimientos y necesidades actuales para la evaluación y gestión del riesgo de la empresa para fines de migración a la tecnología Cloud Híbrida.

Objetivo 2:

Elaborar y diseñar un modelo de evaluación y gestión de riesgo para fines de la implementación de la nueva tecnología Cloud Híbrida.

Objetivo 3:

Determinar la forma en la que se implementaría el cambio a una tecnología cloud híbrida tomando en cuenta la gestión del riesgo tecnológico.

## **CAPÍTULO I. ASPECTOS GENERALES**

### **1.1 Marco Legal**

#### **Introducción**

Esta investigación estará validada según la norma PCI/DSS, la cual proporciona una referencia de requisitos técnicos u operativos desarrollados para proteger los datos de los titulares de tarjetas.

Estas normas se aplican a todas las entidades que participan en el procesamiento de tarjetas de pago, entre las que se incluyen comerciantes, procesadores, adquirentes, entidades emisoras y proveedores de servicios, como también todas las demás entidades que almacenan, procesan o transmiten CHD (datos del titular de la tarjeta) o SAD (datos de autenticación confidenciales).

Las normas PCI/DSS constituyen una serie de requisitos para proteger las informaciones de los titulares de las tarjetas y se pueden mejorar por medio de controles y prácticas adicionales a fin de disminuir otros riesgos de leyes y regulaciones locales, regionales y sectoriales. Además, la legislación o las regulaciones pueden requerir la protección específica de la información de identificación personal u otros elementos de datos (por ejemplo, el nombre del titular de la tarjeta). Las PCI/DSS no sustituyen las leyes locales ni regionales, las regulaciones gubernamentales ni otros requisitos legales.

"A continuación, encontrará una descripción general de los 12 requisitos de las DSS de la PCI."

### Norma de seguridad de datos de la PCI: descripción general de alto nivel

<b>Desarrolle y mantenga redes y sistemas seguros.</b>	<ol style="list-style-type: none"> <li>1. Instalar y mantener una configuración de firewall para proteger los datos del titular de la tarjeta</li> <li>2. No utilizar contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores</li> </ol>
<b>Proteger los datos del titular de la tarjeta</b>	<ol style="list-style-type: none"> <li>3. Proteja los datos del titular de la tarjeta que fueron almacenados</li> <li>4. Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas</li> </ol>
<b>Mantener un programa de administración de vulnerabilidad</b>	<ol style="list-style-type: none"> <li>5. Utilizar y actualizar con regularidad los programas o software antivirus</li> <li>6. Desarrolle y mantenga sistemas y aplicaciones seguras</li> </ol>
<b>Implementar medidas sólidas de control de acceso</b>	<ol style="list-style-type: none"> <li>7. Restrinja el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa.</li> <li>8. Identifique y autentique el acceso a los componentes del sistema.</li> <li>9. Restringir el acceso físico a los datos del titular de la tarjeta</li> </ol>
<b>Supervisar y evaluar las redes con regularidad</b>	<ol style="list-style-type: none"> <li>10. Rastree y supervise todos los accesos a los recursos de red y a los datos de los titulares de las tarjetas</li> <li>11. Pruebe con regularidad los sistemas y procesos de seguridad.</li> </ol>
<b>Mantener una política de seguridad de información</b>	<ol style="list-style-type: none"> <li>12. Mantenga una política que aborde la seguridad de la información para todo el personal.</li> </ol>

Figura 1.1 PCI Security Standards

Fuente: <https://es.pcisecuritystandards.org/>

Adicional a las normas mencionadas, la empresa GSI International se encargará de gestionar un contrato con el cliente interesado, este contrato será generado y validado por el departamento de legal de dicha empresa, donde se especifica cual es el alcance de este proyecto, especificaciones de que esta solución estará en una nube perteneciente a la empresa GSI International y que se le dará el acceso necesario para que el cliente pueda ingresar desde la red en sus servidores. En este documento también se especifica que el cliente tendrá una cantidad de hora disponibles para personalizar esta solución a cómo funciona su negocio, integrarlo con sus sistemas y personalizar la aplicación como desee, dentro de estos cambios el cliente puede tener un margen de un 10% de cambios sin costo alguno adicional, una vez se pase de dicho porcentaje la empresa GSI International procederá a emitir controles de cambios, donde se especificará el alcance de dicho cambio y el costo que conlleva. Posterior a los controles

de cambios, GSI International enviará un acta de cambio donde detalla el cambio que se está realizando, el costo y campos para que los ejecutivos del cliente firme su de acuerdo.

## 1.2 Concepto

En las diferentes conceptualizaciones que han sido escritas para el término de seguridad y evaluación de riesgo, suele establecerse o describirse por sí solo, como las ventajas que nos brinda para poder mitigar cualquier tipo de impacto en un sistema y contar con una contingencia ante cualquier tipo de eventualidad.

La idea del desarrollo de un sistema montado en la tecnología cloud basándose en una gestión y evaluación de riesgo eficaz para la empresa GSI International, ha surgido por diversos motivos, pero el principal y al que se le da prioridad el de poder ofrecer un sistema adecuado a la necesidad de nuestros clientes sobre una plataforma conveniente y customizada y al mismo tiempo garantizar la seguridad e integridad del mismo.

Este tipo de tecnología cloud ofrece las ventajas de que, en el futuro, tienda a ser cada vez más utilizada, por lo que la empresa estaría montándose en una tecnología actual y con tendencia a más desarrollo, lo cual siempre traerá beneficios a la misma, al mismo tiempo, una mejor posición en el mercado al estar a la vanguardia a nivel tecnológico.

El Scope de esta tecnología es mayormente el ahorro, como se menciona anteriormente, se puede llegar a ahorrar entre un 20% y un 30%, teniendo estos porcentajes claros y definidos, la empresa se puede centrar en sus actividades

principales ya que no tendrá el contratiempo de lidiar con equipos tecnológicos físicos, los cuales pueden quitar un mes de todo el año por motivos de reparación y mantenimiento, esto afecta no solo a la normal realización de las tareas, también a los costos.

## **1.2 Historia**

En la actualidad existen diferentes empresas a nivel internacional y nacional que brindan el tipo de tecnología de cloud para fines comerciales y por tanto existe amplia información en la red vinculada a este tema y a la gestión del riesgo tecnológico. Basado en esto tomaremos como referencia algunos de los más destacados para el desarrollo de nuestro tema.

Beltrán, M., y Sevillano, F. (2013) en su libro *“Cloud Computing, tecnología y negocios”* se proponen a estudiar el uso de la tecnología cloud en los negocios y su rápido crecimiento, así como las ventajas e inconvenientes de uso. Para realizaron un levantamiento de informaciones acerca de esta tecnología, así como referencias de otros autores que la han hecho uso de la misma. La conclusión a la que llegaron fue que la tecnología Cloud ha tenido aceptación por su flexibilidad y costo conveniente, también plantearon que los conceptos establecidos en su estudio pueden ser tomados como referencia actual de esta tecnología como para el futuro por personas inclusive que no manejen niveles muy técnicos de informática y se encuentren más orientados al área de negocios.

Vera-Rivera, F., y Pérez-Gutiérrez, B. (2016) en su investigación *“Modelo de Nube Híbrida (Hybrid Cloud) de infraestructura como servicio en el rendimiento de la plataforma SANDBOX - UFPS”* se proponen a estudiar el desarrollo de un modelo de nube híbrida de infraestructura como servicio con el fin de mejorar el rendimiento de la plataforma Sandbox de la Universidad Francisco de Paula Santander (UFPS). Para esto se basaron en el diagnóstico de la tecnología utilizada actual y luego realizaron un sondeo entre proveedores de computación en la nube existentes en el mercado. La conclusión a la que llegaron fue que con este cambio se mejora la disponibilidad, integridad y respaldo de la plataforma, siendo un referente para otras instituciones, empresas en general y para proveedores de infraestructura. Con este tipo de herramientas se automatiza el proceso de despliegue de aplicaciones y bases de datos y facilita el trabajo en equipo.

Céspedes Leguizamón, C. (2016) en su investigación *“Servicios, Amenazas y Gestión del riesgo en la nube”* Se propone a estudiar la forma en la que la tecnología cloud pasó de ser una moda a una necesidad donde las compañías pequeñas pueden acceder a sistemas o tecnología utilizada por grandes empresas tomando en cuenta uso de normas de seguridad. Para ello se sustentó en normativas presentadas por ISACA donde se toman tres renglones principales para fines de gestionar adecuadamente el riesgo. La conclusión a la que llegó fue que existen diferentes recomendaciones a tomar en cuenta para poder eficientizar la gestión de la nube tomando siempre en cuenta proteger la información de alto valor.

Rey-Arenas, N. (2017) en su investigación *“La contratación de servicios de cloud computing: movimientos internacionales de datos y gestión de riesgos de privacidad y seguridad”* Se propone a estudiar los diferentes movimientos internacionales de Datos y leyes aplicables al Cloud Computing. Para ello se sustentó en documentación e informaciones suplidas por los diferentes organismos de jurisdicción y otras directrices vinculadas a l tema. La conclusión a la que llegó es que existen diferentes regulaciones para las informaciones compartidas en el internet a través de la tecnología cloud que, aunque se encuentran vigente pueden no garantizar cien por ciento la seguridad de la información si no se toman las medidas pertinentes.

Bouveret, A. (2018) en su libro *“Cyber Risk for the financial sector: A framework for quantitative assessment”* Se propone a estudiar y generar una documentación novedosa sobre el riesgo cibernético asociado al mundo de las instituciones financieras. Para ello se sustentó en un análisis cuantitativo del riesgo cibernético en las instituciones financieras. La conclusión de este estudio fue la aplicación de un framework en un estándar VaR que puede ser utilizado en diferentes países del mundo donde se puede acceder a diferentes tipos de prácticas de estabilidad de riesgo que pueden implementarse de manera individual y dependiendo el nivel que se requiera, a través de este también es posible visualizar el posible impacto de pérdida financiera antes un riesgo concretizado.

Bouveret, A. (2018) en su libro "*A framework for quantitative assessment*" Se propone a estudiar y generar una documentación novedosa sobre el riesgo cibernético asociado al mundo de las instituciones financieras. Para ello se sustentó en un análisis cuantitativo del riesgo cibernético en las instituciones financieras. La conclusión de este estudio fue la aplicación de un framework en un estándar VaR que puede ser utilizado en diferentes países del mundo donde se puede acceder a diferentes tipos de prácticas de estabilidad de riesgo que pueden implementarse de manera individual y dependiendo el nivel que se requiera, a través de este también es posible visualizar el posible impacto de pérdida financiera antes un riesgo concretizado.

Estas fuentes de información citadas anteriormente serán de ayuda para sustentar de forma teórica y como referencia el estudio que estaremos llevando a cabo en lo adelante con los ejes principales de tecnología cloud, riesgo y las herramientas que intervienen en dicho proceso.

### **Conclusión.**

Como ya antes señalado, la investigación se basó en las normas PCI/DSS, creadas para proporcionar una referencia de requisitos técnicos u operativos desarrollados para la protección de los datos de los titulares de tarjetas de crédito. Estas normas siempre se aplican en todas las entidades que manejan el procesamiento de tarjetas. Por otro

lado, se definió un esquema de conceptos relacionados con seguridad y evaluación de riesgos, para un mejor desarrollo del tema.

Se integró en este capítulo un poco de la historia de la aplicación de tecnologías Cloud en las distintas empresas a nivel nacional e internacional con fines comerciales. Se citaron varios libros como “*Cloud Computing, tecnología y negocios*” de Beltrán, M. y Sevillano, F., “*Servicios, Amenazas y Gestión del riesgo en la nube*” entre otros. Con estas referencias se llevará a cabo el estudio de las tecnologías Cloud, sus riesgos y herramientas.

## **CAPÍTULO II. TECNOLOGÍA CLOUD**

### **Introducción**

En este capítulo se desarrollará la conceptualización de los términos predominantes y más relacionados con la tecnología Cloud, a su vez se estarán definiendo las características, requerimientos, clasificación, ventajas y desventajas de dicha tecnología de manera más amplia, tomando en cuenta la Tecnología Cloud híbrida, la cual es la base y eje de nuestra investigación.

### **2.1 Conceptos Cloud**

Hace referencia a un tipo de arquitectura informática que se define como “una tecnología que permite ofrecer servicios de computación a través de Internet” totalmente (online), básicamente en la nube (Cloud).

### **2.2 Clasificación y características**

Existen tres tipos de nubes:

- Nubes públicas, de uso mundial o global.
- Nubes privadas, son orientadas a soluciones corporativas.
- Nubes híbridas, son una mezcla de las dos nubes anteriores.

## **Tecnología Cloud Pública**

La nube pública está gestionada por terceros que proporcionan servicios en la nube a través de Internet para el público, estos servicios están disponibles como modo de pago por uso.

Ofrecen soluciones para minimizar los costos de infraestructura de TI y actúan como una buena opción para manejar cargas máximas en la infraestructura local. Son una opción de ir a las pequeñas empresas, que pueden iniciar sus negocios sin grandes inversiones iniciales al depender completamente de la infraestructura pública para sus necesidades de TI.

Una característica fundamental de las nubes públicas es la multitenencia. Una nube pública está destinada a servir a múltiples usuarios, no a un solo cliente. Un usuario requiere un entorno informático virtual que esté separado, y muy probablemente aislado, de otros usuarios.

## **Tecnología Cloud Privada**

Las nubes privadas son sistemas distribuidos que funcionan en una infraestructura privada y proporcionan a los usuarios un aprovisionamiento dinámico de recursos informáticos. En lugar de un modelo de pago por uso como en las nubes públicas, podría haber otros esquemas que tengan en cuenta el uso de la nube y la facturación proporcional de los diferentes departamentos o secciones de una empresa.

## **Tecnología Cloud Híbrida**

Una nube híbrida es un entorno informático que combina una nube pública y una nube privada al permitir que se compartan datos y aplicaciones entre ellos. Cuando la demanda de computación y procesamiento tiene cambios, la computación en la nube híbrida brinda a las empresas la capacidad de escalar sin problemas su infraestructura local hasta la nube pública para manejar cualquier desbordamiento, sin dar a otros centros de datos acceso a la totalidad de sus datos.

### **2.3 Requerimientos**

Los requerimientos para adquirir los servicios en la nube, usualmente son los siguientes: Definir el alcance, que esencialmente es definir los límites en que las metas serán las deseadas y los requerimientos de la adquisición de la tecnología cloud. Esta de igual manera, la especificación del proceso de negocio, la cual consiste en una colección de tareas que se relacionan entre sí, diseñadas y agrupadas según las metas del negocio. También tenemos la validación de requerimientos de alto nivel, esto se da una vez que la operación y recursos en la nube se ha verificado, se evalúan los problemas que deben ser resueltos por el consumidor antes de conectarse con el proveedor de la nube. Se analizan los potenciales proveedores, para ver quienes más cubren los requerimientos. Se re-afinan los requerimientos para formalizar los requerimientos que, flexiblemente, puede cubrir el proveedor existente en los entornos de computación en la nube. Se evalúan y negocian los acuerdos del nivel de servicio, se

deben abarcar los puntos tratados del acuerdo de servicio, y si existen, se usa una política de negociación o ajuste. Se documentan y formalizan los requerimientos, para que el proveedor tenga constancia de los requerimientos funcionales, no funcionales y de calidad, asegurando así la trazabilidad y cumplimiento de las metas pautadas.

Continuamos con la Composición del flujo de ejecución, este requerimiento está para asegurar que los servicios, entradas y salidas de las operaciones, configuración de los mensajes entre servicios y los datos, están planificados de forma lógica y coherente con los requerimientos del negocio. Se verifican y validan los requerimientos para descubrir errores, inconsistencias, contradicciones y defectos en los requerimientos que puedan generar caos en la configuración de los servicios. Por último tenemos la Gestión y trazabilidad de los requerimientos, la parte de gestión vela por todo el proceso de ingeniería de requerimientos y la vinculación de los requerimientos con los servicios contratados, la trazabilidad vela porque los requerimientos se consideren y administren a lo largo del acuerdo del servicio, convirtiendo el enfoque en uno iterativo y trazable.

## **2.4 Ventajas y desventajas**

Las características más resaltantes de esta tecnología podrían resumirse en 4: escalabilidad, virtualización, ubicuidad y modelos de pago en función del uso. Ahorro de tiempo y ahorro de costes, y la mejora de la productividad de la empresa. Dicho ahorro de coste se traduce en ahorro de Colaboración, coste de mantenimiento, de coste de inversión, de coste de las licencias de software.

### **2.4.1 Desventajas Tecnología Cloud Híbrida**

Algunas desventajas o lo que más genera preocupación sería la seguridad, la confidencialidad, Pérdida de control de procesos, Dependencia del proveedor, dudas de disponibilidad, responsabilidad del proveedor, dificultad de migración y Costes variables no controlados. Estas son consideradas como las barreras a la hora de usar dicha tecnología: falta de conocimiento, las limitaciones presupuestarias, los costes elevados de contratación, la dificultad de migración, responsabilidad del proveedor, dudas de disponibilidad y dependencia del proveedor.

### **Conclusión.**

En este capítulo se vio todo lo relacionado con la tecnología Cloud, la misma se definió como una tecnología que permite ofrecer servicios de computación a través del internet, totalmente online. Existen 3 tipos de Tecnologías Cloud, que son la Privada, la Pública y la híbrida, ya que la última mencionada es la base de nuestra investigación, se investigó más en torno a la misma, vimos que se define como una mezcla entre la Tecnología Cloud Pública y la privada que permite que se compartan datos y aplicaciones entre ellas. Como todo en la vida, esta tecnología tiene sus ventajas, como la escalabilidad, virtualización, ubicuidad y modelos de pago en función del uso. También tiene sus desventajas como la seguridad, la confidencialidad, dificultad de migración entre otras.

Se puede concluir con que esta tecnología conlleva sus pros y sus contras, pero son más los pros de cara a la mejoría total de cualquier negocio que esté dispuesto a adquirirla.

## **CAPÍTULO III. EVALUACIÓN Y GESTIÓN DEL RIESGO TECNOLÓGICO**

### **Introducción**

En este capítulo estaremos viendo la parte de evaluación y gestión de riesgos tecnológicos, partimos de una definición básica de riesgo y nos vamos adentrando en los demás conceptos. Veremos los controles actuales para llevar todo a cabo de manera exitosa, las amenazas y la seguridad que se debe tener en cuenta, también se la gestión de riesgos en la Tecnología Cloud Híbrida, el foco de investigación. Las herramientas de seguridad forman parte de este capítulo, así como la integración con otros servicios, detallada con imágenes que hacen más fácil el entendimiento.

### **3.1 Conceptos**

#### **3.1.1 Definición Evaluación**

Consiste en verificar un proceso o sistema para detectar y conocer las deficiencias y problemas que éste presenta.

#### **3.1.2 Riesgo**

El riesgo es una probabilidad de que ocurra un hecho que pueda ocasionar algún tipo de daño o pérdida.

#### **3.1.3 Riesgo Tecnológico**

El riesgo tecnológico es una vulnerabilidad que puede estar presente tanto en la infraestructura (hardware) como en la parte lógica o de sistemas, también es el uso inadecuado de dichos factores.

### **3.1.4 Evaluación de Riesgo Tecnológico**

La evaluación de riesgo es un elemento clave para la planificación de la acción preventiva en una empresa, puesto que a partir de ella se elaborarán y desarrollarán las medidas de protección y corrección que crearán unas condiciones de seguridad y salud adecuadas.

Para evaluar el riesgo tecnológico, debemos saber: si la tecnología utilizada está suficientemente controlada.

- si la vida del proyecto es o no sustancialmente superior al plazo de la financiación otorgada (concepto cola).
- si la planta o instalaciones producidas se han proyectado de manera que puedan seguir siendo competitivas a lo largo del tiempo.
- si existe disponibilidad de piezas y partes críticas para posibles eventualidades.

El caso de que las cuatros premisas anteriores tengan una respuesta afirmativa, las entidades financieras aceptaran el riesgo técnico.

### **3.1.5 Controles**

Consiste en una revisión periódica de un proceso, sistema, herramienta, etc. para fines de comprobar su correcto funcionamiento en relación a un objetivo pautado y de manera posterior realizar cualquier ajuste o corrección.

### **3.1.6 Amenaza**

Consiste en un posible riesgo, puede estar considerado en estas fallas en sistemas, accidentes, procedimientos, desastres naturales, etc.

### **3.1.7 Seguridad**

La seguridad mayormente es definida como la falta de cualquier tipo de peligro que pueda ocasionar daño físico, psicológico o de cualquier tipo de infraestructura, básicamente existen para asegurar la integridad física, emocional y estructural de individuos y del entorno.

### **3.1.8 Riesgo tecnológico orientado a servicios Cloud**

El riesgo orientado a Servicio Cloud, abarca 4 campos, que son: confidencialidad, disponibilidad, integridad y portabilidad de datos. Esto se debe a que a través del Cloud se arriesga a que se encuentren disponibles informaciones de mucha importancia para las empresas que usan este servicio, esto se sustenta partiendo de que actualmente, la información es lo más valioso que tiene una empresa.

### **3.1.9 Herramientas para seguridad**

Toda tecnología es vulnerable de ataques y fallas, para esto se crearon herramientas y/o sistemas para garantizar la seguridad e integridad de los datos. Tenemos muchas de bastante utilidad a la hora de protegerse de cualquier amenaza posible, a continuación, se mencionan algunas. Están los sistemas de identificación, como contraseñas, datos biométricos, entre otros para restringir y controlar el acceso a la seguridad. También los Firewalls, que sirven para controlar lo que entra y sale de una red. A su vez están los sistemas de detección de intrusos que permiten detectar muchos tipos de ataques y alertan sobre ellos.

### **3.1.10 Integración con otros servicios**

La solución de verticales en las nubes, como se había mencionado, está construida en Bizagi, el mismo provee una muy buena capa de integración que soporta las diferentes posibilidades de integración para las soluciones corporativas desarrolladas en el estándar BPM.

En estas soluciones donde se requiere integrar con otras aplicaciones o servicios existentes, la capa de integración de Bizagi presenta múltiples opciones de integración, útiles tanto como opciones de integración a nivel de datos, o a nivel de proceso (integración con servicios).

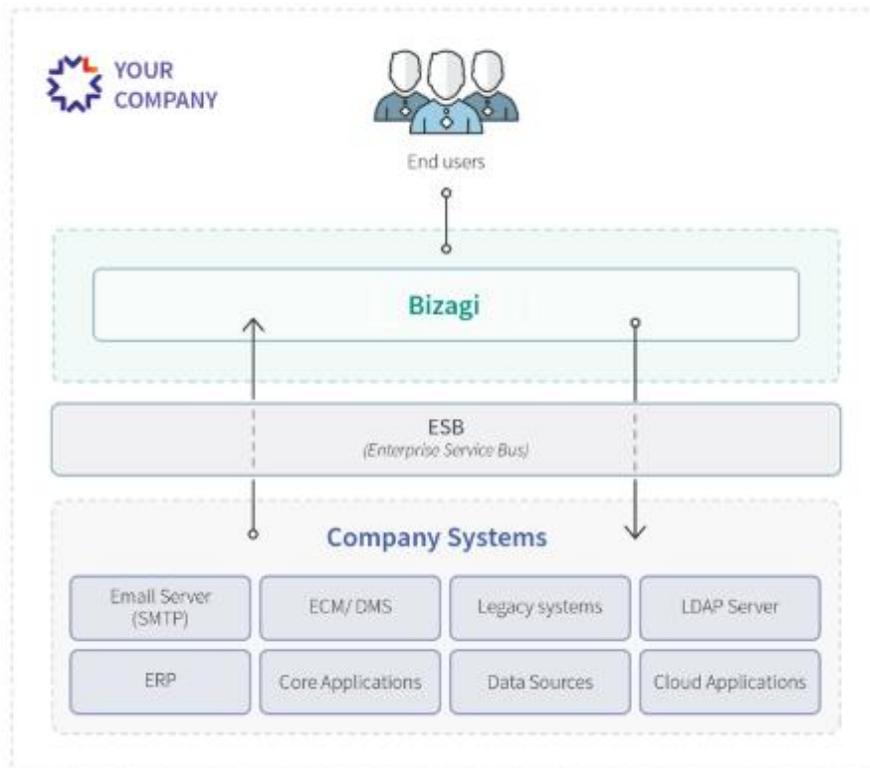


Figura 1.2 BPM Suite, Entorno Bizagi  
Fuente: [https:// help.bizagi.com](https://help.bizagi.com)

Adicional a las integraciones que habíamos mencionado anteriormente bizagi también puede realizar réplicas de tablas en otras bases de datos, esto funciona para no tener que registrar un producto en ambos sistemas o agregar registros en una tabla que puede cambiar, sino que cada x tiempo bizagi replique esta tabla y obtenga dicha información directamente desde esa base de datos, estas réplicas pueden ser usadas solo para entidades paramétricas.

Otras de las formas que tiene bizagi para integrarse a nivel de datos es la virtualización de tablas, que en definitiva hace lo mismo que las réplicas, pero esto solo para entidades maestras, de manera que si tengo un listado de datos que necesito de una base de datos x puedo usar esta información en nuestra aplicación.

La capa SOAP que utiliza bizagi es en ambas direcciones, podemos tanto integrarnos con otros sistemas cómo hacer que su sistema obtenga datos desde bizagi, para esto bizagi en su capa SOAP pública servicios web que pueden ser consumidos por otra aplicación, esto para realizar diversas funciones tales como crear un nuevo caso, guardar información, darle a siguiente a un caso en curso, cancelar una solicitud, entre otras cosas.

## **Conclusión**

En este capítulo se tocaron varias definiciones, tales como riesgo, que es plenamente la probabilidad de que ocurra un hecho que perjudique o que provoque algún daño, en ese mismo orden está el riesgo tecnológico, es básicamente igual al riesgo, pero con la variable Hardware y Software, amenazas a los mismos que puedan afectar su funcionamiento y la integridad de los datos de cualquier sistema. La evaluación de riesgos tecnológicos es muy importante y siempre debe tomarse en cuenta, ya que es un elemento clave para la planificación de la acción preventiva en una empresa, a partir de ella se elaboran las medidas de protección y corrección que servirán para formular nuevas condiciones de seguridad.

Otros aspectos importantes son los controles, amenazas y seguridad en la evaluación de riesgos. Siguiendo nuestra línea de investigación, la gestión y evaluación de riesgos tecnológicos orientado a Cloud es crucial ya que la misma puede tener un riesgo de exposición de datos muy alto, y como sabemos, la información es lo más valioso en este entorno. Las herramientas de seguridad son muy importantes, tales como firewalls, datos biométricos, contraseñas y algunas que permiten detectar ataques y alertar sobre ellos.

Mencionar la integración con otros servicios también es importante, tales como Bizagi, este sistema provee una buena capa de integración que soporta las distintas vertientes de integración para las soluciones corporativas desarrolladas en el estándar BPM.

## **CAPÍTULO IV. HERRAMIENTAS Y SOLUCIONES PARA NEGOCIOS**

### **Introducción**

En este capítulo se va a hablar sobre las herramientas y soluciones para negocios, se verán las herramientas usadas en Cloud en general tales como BPMN, BPMI, Bizagi. Se va a definir qué es BPM y las herramientas basadas en este software, para un mayor entendimiento de este capítulo. Por consiguiente, se van a tratar las normas PCI/DSS, que son una parte fundamental en el proceso de pagos por tarjeta de crédito.

### **4.1 Conceptos de las Herramientas**

Business Process Model and Notation (BPMN), en español Modelo y Notación de Procesos de Negocio, es una notación gráfica estandarizada que permite el modelado de procesos de negocio, en un formato de flujo de trabajo (workflow). BPMN fue inicialmente desarrollada por la organización Business Process Management Initiative (BPMI), y es actualmente mantenida por el Object Management Group (OMG), después de la fusión de las dos organizaciones en el año 2005.

#### **4.1.2 BPM**

El BPM se puede definir como una nueva categoría de software empresarial que permite a las empresas modelar, implementar y ejecutar varias actividades interrelacionadas –es decir, Procesos– de cualquier naturaleza, ya sea dentro de un departamento o permeando la entidad en su conjunto, con extensiones para incluir a los clientes, proveedores y otros agentes como parte de las tareas en los procesos.

#### **4.1.3 Bizagi**

BizAgi es la solución BPM que le permite a usted y a su organización diseñar, modelar, integrar, automatizar y monitorear sus procesos comerciales a través de un gráfico ambiente. Es la forma más rápida y eficiente de lograr la continua mejora de sus procesos.

#### **4.1.4 Norma PCI/DSS**

El estándar de seguridad de tarjetas de pago PCI DSS ha tenido en los últimos años un auge derivado tanto de la gran cantidad de fraudes con tarjetas, como de la creciente presión regulatoria de las marcas de tarjetas sobre los comercios. Esta guía pretende, con un lenguaje sencillo y accesible, explicar desde el inicio los conceptos generales de PCI DSS de tal manera que el lector sea capaz de comprender su aplicabilidad, requisitos, cadena de supervisión y estrategia de implantación.

#### **4.1.5 Capa SOAP**

Los servicios SOAP de Bizagi son uno de las dos APIs para acceso programático desde aplicaciones externas, como se describe en API de Bizagi.

Los métodos web de la Capa SOAP están agrupados dentro de las siguientes categorías, de acuerdo al servicio que representa un componente principal de la arquitectura de producto de Bizagi.

#### **Conclusión**

Al terminar este capítulo podemos concluir que todo lo relacionado con BPM es importante ya que este permite modelar, implementar y ejecutar varias actividades interrelacionadas, en otras palabras, procesos de cualquier naturaleza. Una de las herramientas más usadas es Bizagi, por su forma rápida y eficiente de lograr la continua mejora de los procesos.

Enfocados en este proyecto, definimos las normas PCI/DSS y su importancia, ya que el auge de los fraudes en tarjetas de crédito en estos tiempos es bastante evidente. En el mismo orden se trató la capa SOAP, los servicios de la misma son una de las dos APIs para acceso pragmático desde aplicaciones externas.

## **CAPÍTULO V. SISTEMA**

### **Introducción**

A continuación, se definirán lo que es Software, Base de Datos y Servidores, todos herramientas importantes y parte fundamental de cada empresa o negocio. Los softwares facilitan cualquier proceso, las bases de datos nos permiten manejar bastante grandes cantidades de datos, veámoslo más a fondo a continuación.

### **5.1 Software**

El software es un conjunto de documentos asociados y la configuración de datos requeridos para hacer que los programas operen de manera correcta. Generalmente estos sistemas consisten en múltiples programas independientes, también de archivos de configuración utilizados para la ejecución de dichos programas, sistemas de documentación que lo describen y explican al usuario.

### **5.2 Base de Datos**

La base de datos no es más que una estructura computarizada compartida que guarda datos de interés para el usuario final, y se maneja lo que es metadatos, básicamente, datos sobre datos y a través de estos los datos del usuario final son manejados e integrados acorde a lo que se está realizando. Para mejor entendimientos, los metadatos dan una descripción de las características de los datos y de sus relaciones, las cuales enlazan lo mismos contenidos en la base de datos.

### **5.3 Servidores**

“Un servidor es una aplicación en ejecución de software preparado para atender las peticiones de un usuario o cliente y devolverle una respuesta en servicio solicitada, los servidores se los pueden hacer ejecutar en cualquier computadora, incluso en computadores dedicados en lo que en la mayoría se los conoce individualmente como servidor". (informaticamoderna, 2015).

Mayormente un servidor puede brindar muchos servicios y tener a disposición varios servidores que funcionen a la misma vez, lo cual siempre es recomendado para tener el servidor en las computadoras que brindan su uso como una medida de seguridad. Usualmente los servidores prestan sus servicios en empresas que adquieren estos para sus usuarios y también está para el público en general a través de internet.

### **Conclusión**

Al concluir este capítulo podemos decir que el software es un conjunto de documentos asociados y una configuración de datos requeridos para hacer que los programas operen de manera correcta. Sabemos también que las bases de datos no son más que estructuras computarizadas compartidas que guardan datos de interés para el usuario final, desde lo más mínimo hasta lo más detallado, todo depende de lo que se busque o de los requerimientos de cualquier programa. Con certeza podemos decir que un servidor es una aplicación de software preparada para atender las peticiones de cualquier usuario o cliente y retornar una respuesta en servicio solicitada. Todos estos

elementos son importantes a la hora de llevar a cabo satisfactoriamente las operaciones de cualquier negocio o empresa.

## **CAPÍTULO VI. METODOLOGÍA**

### **Introducción**

En este capítulo se va a definir la metodología usada en esta investigación y las definiciones que van de la mano con la misma, se dará una breve definición de y se estará desarrollando el tipo de investigación usada en nuestro proyecto, al igual que los métodos. A continuación, veremos la población definida y muestra para este proyecto.

### **Metodología**

Méndez lo define como “el procedimiento riguroso, formulado de una manera lógica, que el investigador debe seguir en la adquisición del conocimiento”.

#### **6.1 Tipos de investigación**

El tipo de investigación que se utilizará será una combinación tanto del enfoque cuantitativo como el del cualitativo, este es llamado enfoque mixto, definido por Hernández Sampieri (2010) como “un proceso de recolección que implica el análisis y vinculación de datos cuantitativos y cualitativos en un mismo estudio o una serie de investigaciones para responder a un planteamiento del problema”. Dando hincapié a que el objetivo de este enfoque no es el de sustituir a ninguna de las otras dos, sino utilizar, reunir las ventajas y beneficios de cada una

Es una investigación descriptiva debido a que se muestran las características, propiedades o rasgos que puedan ser relevantes para la investigación y explicativa porque busca instituir las causas de cada modalidad o del sistema y así poder tener un mejoramiento al hacer el cambio y brindar un servicio de más calidad.

El propósito general de la investigación es buscar una alternativa adecuada para el uso de tecnología cloud teniendo así una gestión de riesgos tecnológicos acertada, para brindar un mejor servicio a los clientes de la empresa mencionada, establecer los parámetros necesario que se necesitan para llevarlo a cabo a través de una serie de procedimientos y puntualizando los más relevantes para un mejor entendimiento de su importancia.

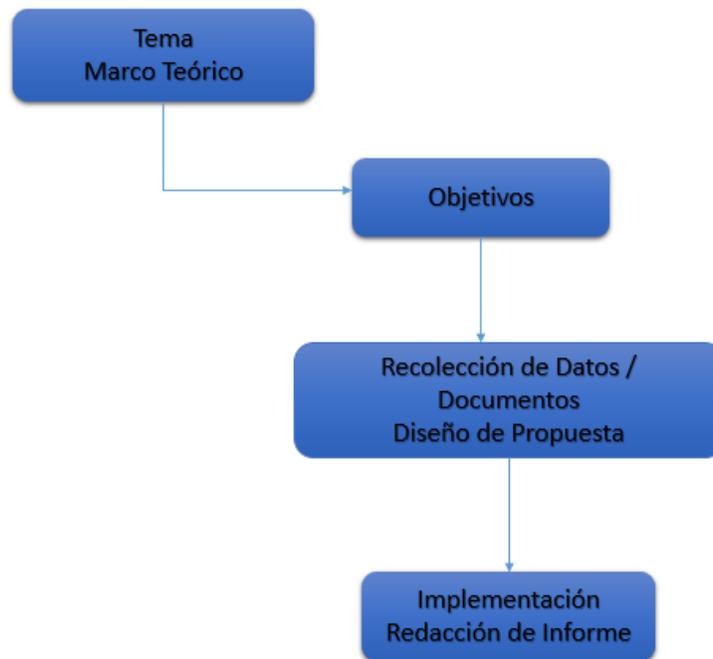
## **6.2 Métodos**

En este trabajo los métodos de muestreo existente para realizar la investigación se dividirán en cuatro (4) fases, de esta manera podemos llevar la investigación de una forma más organizada, clara y limpia. Estas mismas fases están predeterminadas en las fases que frecuentemente se utilizan para las investigaciones.

En la primera fase es donde se da inicio a la definición del tema que se está investigando, realizar un marco teórico en donde claramente se exprese la conceptualización de los términos, se realiza la toma de decisiones entorno a los instrumentos o procedimientos que se llevarán a cabo para realizar la investigación del Sistema.

En la segunda fase damos a conocer los objetivos que se buscan al realizar el cambio a una tecnología cloud híbrida y de esta forma asegurar que la implementación de esta traiga consigo un cambio positivo y que aporte calidad, dando conocer en estos objetivos la relevancia del tema en cuestión.

La tercera fase es en donde recolectamos todas las informaciones, datos y análisis y al recolectarlos, iniciamos el proceso de desarrollo de la investigación, puntualizando los temas importantes para así obtener un mejor entendimiento sobre este. Se evalúan las recomendaciones y conclusiones. Procedemos a compactar y concluyendo, en la última o cuarta fase, se procede a realizar una propuesta sobre el cambio de tecnología.



### **6.3 Población y Muestra.**

Tamayo y Tamayo (1997) define población como “la totalidad del fenómeno a estudiar en donde las unidades de población poseen una característica en común, la cual se estudia y da origen a los datos de la investigación”. “Es el conjunto de elementos de referencia sobre el que se realizan las observaciones.” (Rivas,2012).

Para un mejor entendimiento se puede exponer como una serie de determinadas características en común, dentro de un conjunto.

La muestra a su vez es definida por Tamayo y Tamayo como los elementos que seleccionamos con la intención de averiguar algo sobre la población. Es decir, que la muestra viene siendo el instrumento o los métodos que utilizamos para realizar la investigación sobre la población.

Para este trabajo estaremos tomando como muestra una población del sector bancario que hace uso de transacciones para fines de realizar procesos de crédito y tarjetas, la idea con esto es a través de una encuesta poder validar si tendría acogida la proposición de un sistema en la nube customizable y de esa forma ver su posible aceptación por parte de los clientes de la empresa y utilizar esta condición como trampolín.

## 6.4 Técnicas e Instrumentos

Según Martínez Godínez (2013) “la técnica propone las normas para ordenar las etapas del proceso de investigación, de igual modo, proporciona instrumentos de recolección, clasificación, medición, correlación y análisis de datos, y aporta a la ciencia los medios para aplicar el método. Las técnicas permiten la recolección de información y ayudan al ser del método.” (p. 4).

Otra manera de describir las técnicas de investigación es el medio que se utiliza el cual funciona como un eje fundamental es lo que es la recolección de los datos, documentos, etc. Este nos orienta en el proceso de la captación de instrumentos a utilizar.

Méndez (2001) expresa que: “Las fuentes son hechos o documentos a los que acude el investigador y que le permiten obtener información” Según el autor se dividen en fuentes primarias (Observación, encuestas, cuestionarios, entrevistas, sondeos) y secundarias (textos, revistas, documentos, prensa, otros). En esta investigación se estarán realizando las dos fuentes en conjuntos para así poder obtener un mejor resultado para un sistema más eficiente.

Para nuestra investigación estaremos utilizando como una de las herramientas la encuesta, que en este caso decidimos realizarla a los clientes que actualmente utilizan los servicios tecnológicos que son brindados por la empresa de manera convencional, con esto estaremos determinando la duración del proceso actual y cómo estos procesos se pueden ver afectados de manera positiva realizando su migración a las nubes.

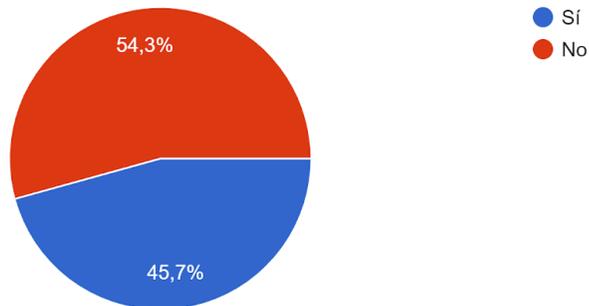
Ver a continuación resultados de acuerdo a la encuesta adjunta (anexos):

**Población seleccionada:** Sector Bancario

**Muestra:** Usuarios de sistemas para solicitud de tarjetas de créditos y prestamos

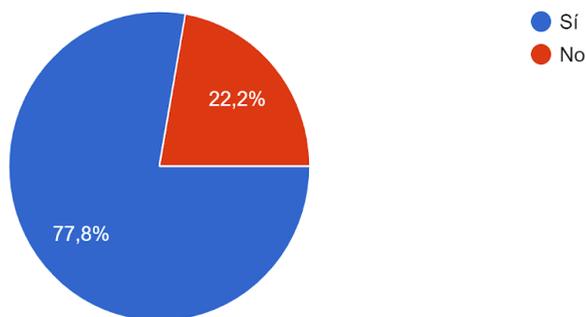
¿Conoce usted la Notación BPMN?

35 respuestas



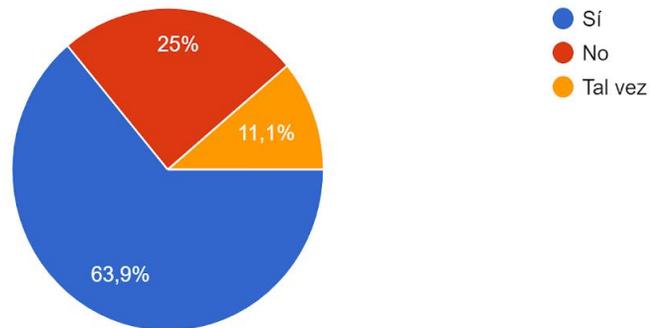
¿Conoce o ha escuchado sobre Bizagi?

36 respuestas



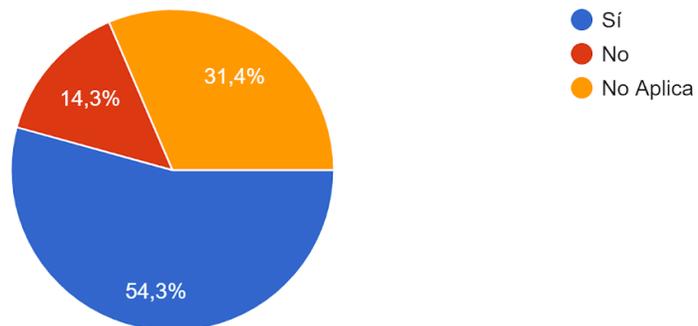
¿Ha escuchado sobre las soluciones en las nubes?

36 respuestas



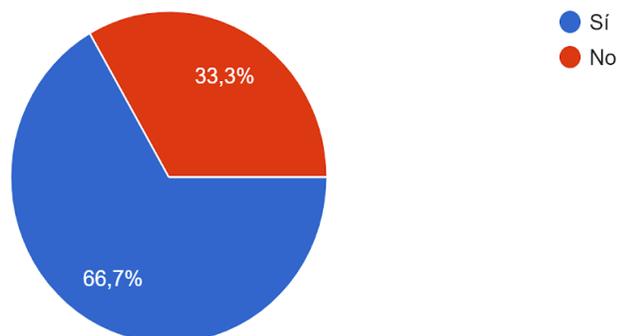
¿En caso de que su respuesta sea No, está dispuesto a adquirir un sistema automatizado para esta gestión?

35 respuestas



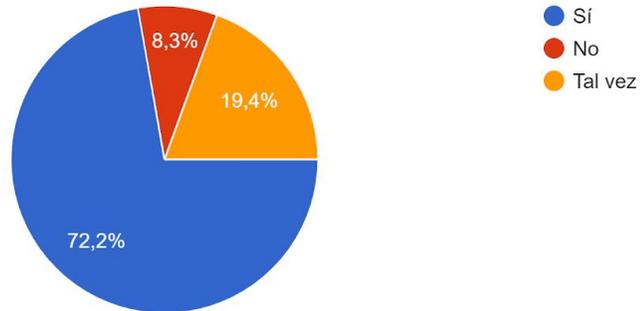
¿Cuenta usted en la actualidad con un sistema para gestionar las solicitudes de tarjetas de crédito y préstamos?

36 respuestas



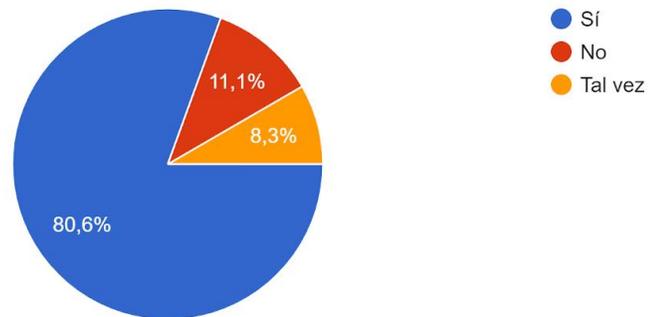
¿Le interesaría tener una aplicación de esta magnitud en las nubes?

36 respuestas



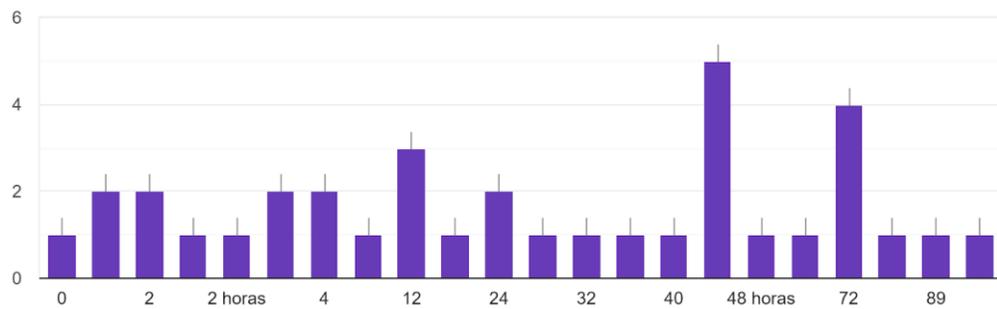
¿Le interesaría tener acceso a esta aplicación desde su teléfono móvil?

36 respuestas



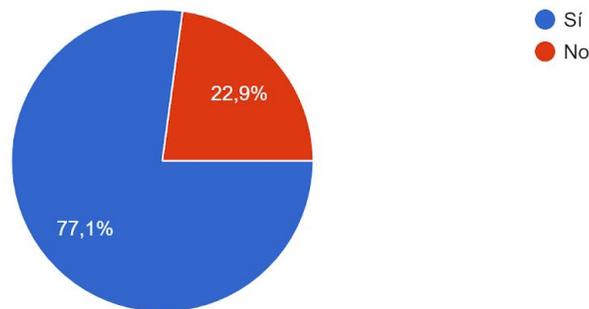
¿Qué cantidad de tiempo aproximado (en horas) en horas dura una solicitud en sus sistemas actuales?

36 respuestas



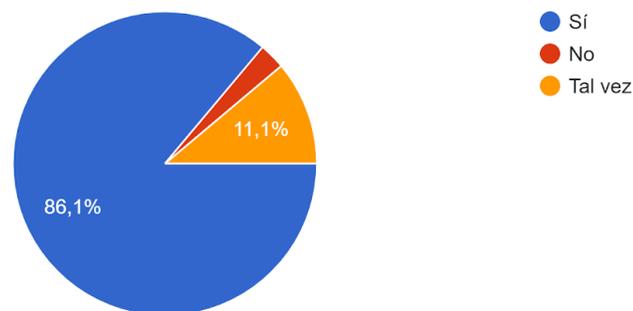
¿Entiende usted que los procesos actuales pueden ser optimizados con una solución en las nubes bajo la notación de BPMN?

35 respuestas



¿Estaría dispuesto(a) a recibir una prueba de concepto de estas verticales para ver el valor que le aportaría a su empresa?

36 respuestas



*Figura 1.3 Encuesta*  
*Elaboración: Propia*  
*Fuente: <https://surveys.google.com>*

Adicional a esta recopilación, actualmente esta solución se lleva a cabo en un servidor en las instalaciones GSI International, a este se le realiza un backup a un servidor secundario en las nubes para proteger la información, cuando se gestione el pase a producción esta solución estará alojada en un servidor de azure y se le estará programando un backup diariamente en horario nocturno. La empresa cuenta con un servicio antivirus Kaspersky y lo tiene alojado en este servidor, en cuanto a la seguridad

que tiene el mismo son los que azure nos ofrece en sus paquetes y los cuales detallaremos a continuación:

### **Uso de Controles de redes sólidos**

Se conectarán las máquinas virtuales y los dispositivos de Azure a otros dispositivos en red, colocándolos en redes virtuales de Azure. En definitiva, podremos conectar tarjetas de interfaz de red virtual a una red virtual para posibilitar las comunicaciones basadas en TCP/IP entre dispositivos habilitados para la red. Las máquinas virtuales conectadas a una red virtual de Azure pueden conectarse a dispositivos en la misma red virtual, en distintas redes virtuales, en Internet o, incluso, en sus propias redes locales, con esto lograremos poder acceder a la aplicación desde incluso dispositivos móviles.

### **Alta disponibilidad**

Estos servidores tendrán un conjunto de tecnologías que minimizan las interrupciones de TI al proporcionar una continuidad empresarial de los servicios de TI mediante componentes redundantes, con tolerancia de errores o protegidos mediante conmutación por error dentro del mismo centro de datos. En nuestro caso, el centro de datos se encuentra en una región de Azure.

## Protección contra DDoS

Además de las medidas de seguridad básica que tendremos con firewall y los segmentamientos de red también contaremos con el servicio de Azure DDoS Protection Standard el cual proporcionará las funcionalidades avanzadas de mitigación contra DDoS ante ataques en la red. La misma se ajustará automáticamente para proteger los recursos específicos de Azure.

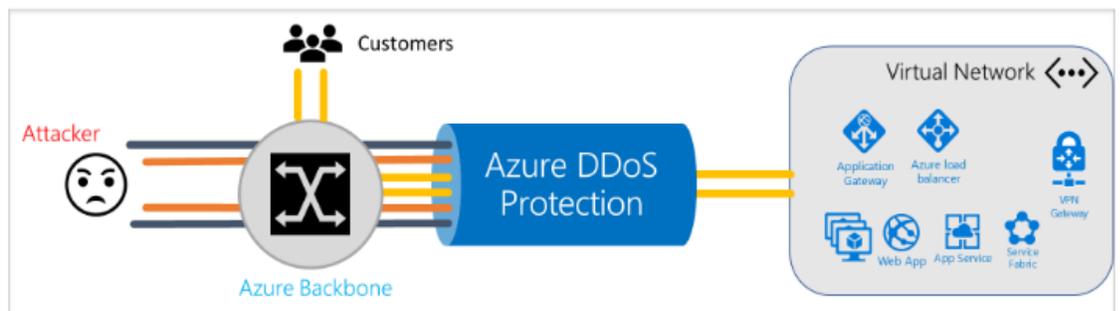


Figura 1.4 Ilustración Azure DDoS Protection

Fuente: <https://docs.microsoft.com/en-us/azure/security/fundamentals/ddos-best-practices>

## Escalabilidad de carga

La escalabilidad representa el grado en que un sistema puede controlar el aumento de la carga. Nuestro sistema está diseñado de modo que se puede escalar horizontalmente para satisfacer la demanda de una carga mayor, específicamente en caso de un ataque de DDoS. En nuestro caso usaremos el servicio Azure Cloud Services, el cual se configura cada uno de los roles para utilizar varias instancias. Azure nos

recomienda usar conjuntos de escalado de máquinas virtuales para contar con funcionalidades de escalado automático

Por otra parte, se han enumerado desde la parte de seguridad posibles riesgos al adoptar este cambio de servicio a la nube y su probabilidad x impacto.

1. Seguridad.
2. Disponibilidad.
3. Riesgos de Virtualización.
4. Recuperación de desastre.
5. Dependencia para manejo de un tercero o falta de control.
6. Se comparte la infraestructura con más organizaciones.
7. Protección de datos (acceso a datos no autorizados).

**(Probabilidad x Impacto).**

Seguridad



### Disponibilidad



### Riesgo de virtualización



### Recuperación de desastre



### Dependencia de manejo tercero o fa...



### Infraestructura compartida con más ..



### Protección de datos ( acceso a dato...



Figura 1.5 Matriz efectiva Gestión de Riesgo (Gráficas Probabilidad x Impacto)  
Fuente: <https://www.cleolevel.com>

## **Seguridad**

Restringir estrictamente el acceso. Examinar regularmente los niveles de acceso de los usuarios y validar si están de acuerdo al uso. Reducir súper usuarios o administradores, tener solo los necesarios.

## **Disponibilidad**

Hacer uso de la política de seguridad del servicio en la nube para mantener la disponibilidad de la misma.

## **Riesgos de Virtualización.**

La mayoría de los productos de virtualización soportan la creación de conmutadores de red virtuales y configuraciones de red como parte del entorno. Así mismo, soportan la creación de subredes privadas para la comunicación entre las máquinas virtuales alojadas en un mismo servidor. Este tráfico no puede ser monitorizado por los elementos físicos típicos de la red por ello, se deben tener más precauciones de la seguridad de la red en estas conexiones internas para evitar ataques desde dentro de estas redes virtuales.

## **Recuperación de Desastre**

Utilizaremos la recuperación de desastres en la nube (DR en la nube o Cloud DR) que es una estrategia de respaldo y restauración que consiste en almacenar y mantener copias de registros electrónicos en un entorno de computación en la nube como medida de seguridad.

## **Dependencia para manejo de un tercero o falta de control**

Optar por obtener servicios de empresas certificadas con experiencia y alta disponibilidad para reducir este riesgo.

## **Se comparte la infraestructura con más organizaciones**

Este riesgo es mínimo puesto que el proveedor garantiza la protección y accesibilidad de los datos e informaciones de cada empresa, a su vez permite reducción de costes al ser un hardware compartido. Sugerimos para mitigar cualquier posibilidad de amenaza contar con un empresa certificada y reconocida en estos servicios.

## **Protección de datos**

Al proveedor responsable de los ficheros y de su tratamiento le corresponde garantizar mediante el contrato de prestación de servicios de tratamiento de datos personales por cuenta de terceros suscritos que dicho servicio se recibe con todas las garantías técnicas y de protección de información.

## CONCLUSIÓN Y RECOMENDACIONES

La metodología es el procedimiento riguroso formulado de una manera lógica que el investigador debe seguir en la adquisición del conocimiento. Como se explicó, usaremos una combinación del enfoque cuantitativo y el cualitativo, en otras palabras, un enfoque mixto, que no pretende sustituir ningún enfoque, más bien utilizar las ventajas de ambos. El método utilizado está dividido en cuatro fases, en la primera se define el tema, en la segunda se dan a conocer los objetivos de la investigación, la tercera es la de recolección de datos, información y análisis, y en la última fase es la de proponer los cambios planteados en la investigación.

Sobre la población se encontró que esta es la totalidad del fenómeno a estudiar donde las unidades de población poseen una característica en común y la muestra se define como los elementos que tomamos con la intención de averiguar algo sobre la población, con estos dos métodos recolectamos información del sector bancario que hace uso de las transacciones para fines de realizar procesos de crédito y tarjetas,

Se han enumerado posibles riesgos al adoptar este servicio Cloud con la posibilidad por impacto y se tomó en cuenta lo siguiente: Seguridad, Disponibilidad, Riesgo de Virtualización, Recuperación de Desastre, Dependencia para manejo de un tercero o falta de control, compartir infraestructura con más organizaciones y protección de datos, es decir el acceso a datos no autorizado.

Luego de analizar los datos que hemos recopilado en esta investigación hacemos las siguientes recomendaciones:

- 1-** No utilizar contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores.
- 2-** Proteger los datos del titular de la tarjeta que fueron almacenados.
- 3-** Cifrar la transmisión de los datos del titular de la tc en las redes públicas abiertas.
- 4-** Realizar una integración entre el sistema y un certificado de seguridad.
- 5-** Rastrear y supervisar todos los accesos a los recursos de red y a los datos de los titulares de las tarjetas de crédito.
- 6-** Mantener políticas que aborden la seguridad de la información para todo el personal.
- 7 -** No permitir que se almacene los datos confidenciales de la tc como el Pin/bloqueo, el cvc2 y el cvv2.
- 8-** Implementar un monitoreo constante de los controles de seguridad, tales como firewalls, IDS/IPS (sistemas de intrusión-detección o de intrusión-prevención), FIM

(monitorización de la integridad de archivos), antivirus, controles de acceso, etc., para asegurarse de que funcionan correctamente y según lo previsto.

**9-** Garantizar la detección de todas las fallas en los controles de seguridad y solucionarlas oportunamente. Los procesos para responder en caso de fallas en el control de seguridad son los siguientes:

- Restaurar el control de seguridad.
- Identificar la causa de la falla.
- Identificar y abordar cualquier problema de seguridad que surja durante la falla del control de seguridad.
- Implementar la mitigación (como procesos o controles técnicos) para evitar que la causa reaparezca.
- Reanudar la monitorización del control de seguridad, quizás con una monitorización mejorada durante un tiempo a fin de verificar que el control funcione correctamente.

**10-** Revisar los cambios implementados en el entorno (por ejemplo, incorporación de nuevos sistemas, cambios en las configuraciones del sistema o la red) antes de finalizar el cambio y realizar las siguientes actividades:

- Determinar el posible impacto en el alcance de las PCI DSS (por ejemplo, una nueva regla para los firewalls que permita la conectividad entre un sistema del CDE y otro sistema puede incorporar sistemas o redes adicionales al alcance de las PCI DSS).
- Identificar los requisitos de las PCI DSS correspondientes a los sistemas y las redes afectados por los cambios (por ejemplo, si un nuevo sistema está dentro del alcance de las PCI DSS, se deberá configurar de acuerdo con las normas de configuración de sistemas, entre otros, FIM (monitorización de la integridad de archivos), AV (antivirus), parches, registros de auditorías, etc., y se deberá incorporar al programa trimestral de análisis de vulnerabilidades).

**11-** Revisar las tecnologías de hardware y software, al menos, una vez al año para confirmar que el proveedor las sigue admitiendo y que pueden satisfacer los requisitos de seguridad de la entidad, incluso las PCI DSS. Si se detecta que el proveedor ya no puede admitir las tecnologías o que no pueden satisfacer las necesidades de seguridad de la entidad, la entidad debe preparar un plan de recuperación que incluya el reemplazo de la tecnología si fuera necesario.

## BIBLIOGRAFÍA

Object Management Group, Inc. (1997-2020). *Object Management Group Business Process Model and Notation*. Object Management Group. Recuperado de <http://www.bpmn.org/>

Beltrán, M. Sevillano, F. (Enero 1, 2013). *Cloud Computing, Tecnología y Negocio*. Ediciones Paraninfo, S.A. Recuperado de <https://books.google.com.do>

Vera-Rivera, F, H. Perez-Gutierrez, B, R. Urbina, V, M. (2016). *MODELO DE NUBE HÍBRIDA (HYBRID CLOUD) DE INFRAESTRUCTURA COMO SERVICIO PARA MEJORAR EL RENDIMIENTO DE LA PLATAFORMA SANDBOX - UFPS*. Conferências Ibero-Americanas WWW/Internet e Computação Aplicada. Recuperado de <https://www.researchgate.net>

Céspedes, C, A. (s.f). *SERVICIOS, AMENAZAS Y GESTIÓN DEL RIESGO EN LA NUBE*. Universidad Piloto de Colombia. Recuperado de <http://polux.unipiloto.edu.co>

EcuRed. (s.f). *Tecnología de Nube*. EcuRed. Recuperado de <https://www.ecured.cu>

Microsoft. (2020). *¿Qué es una nube híbrida?*. Microsoft Azure. Recuperado de <https://azure.microsoft.com>

Zabala-Vivanco, J. Rio-Belver, R. Cilleruelo-Carrasco, E. Garechana-Anacabe, G. Gavilanes-Trapote, J. (Junio, 2013). *Beneficios del Cloud Computing para la Pequeña y Mediana Empresa*. Technology Foresight Management (TFM). Recuperado de <https://www.researchgate.net>

Auraportal. (Anexo I. Anteproyecto 2020). *¿Qué es BPM?*. Miami, E.U.: Auraportal. Recuperado de <https://www.auraportal.com>

Goetz, M. (s.f). *Modeling Workflow Patterns through a Control-flow perspective using BPMN and the BPM Modeler BizAgi*. Institute of Applied Informatics and Formal Description Methods University Karlsruhe (TH). Recuperado de <http://wiki.recife.pe.gov.br>

Ferrini-Fonseca, D. (2019). *PCI Dss, Breve Guía Para El Cumplimiento*. Publicado Independientemente. Recuperado de <https://books.google.com.do>

Bizagi. (2002-2020). *Servicios web SOAP*. Bizagi. Recuperado de <http://help.bizagi.com>

Casanovas, T. (2016). *Project Finance International*. Barcelona, España.: Profit Editorial. Recuperado de <https://books.google.com.do>

Sommerville, I. (2005). *Ingeniería del software*. Pearson educación. Recuperado de <https://books.google.es>

Coronel, C., Morris, S., & Rob, P. (2011). *Base de datos: diseño, implementación y administración*. Cengage Learning Editores. Recuperado de <https://books.google.es>

Cedeño, R. L. F. (2016). *Consolidación de servidores mediante la virtualización (Master's thesis, Quito: Universidad Israel, 2016)*. Recuperado de <http://157.100.241.244>

**ANEXOS****ANEXO I - Anteproyecto**

**VICERRECTORÍA ACADÉMICA  
OFICINA COORDINADORA DE CURSO MONOGRÁFICO**

**Anteproyecto del Trabajo Final (TF) en la modalidad de Monografía Investigación  
Acción para optar por el título de**

Ingeniería en Sistemas de Información

**Título de la monografía:**

Evaluación de Riesgos y Controles para el uso de Tecnología Cloud Híbrida en GSI  
International.

<b>Nombres estudiantes</b>	<b>Matriculas</b>
María Teresa Ciriaco	2008-1736
Eliseo Santana	2011-1552
Edgar Payano	2012-2445

**Nombres de los profesores del Conferencista y el Auxiliar**

Nirka Hernández y Willy Padua

**INDICE**

<b>Título del Tema</b>	<b>3</b>
<b>Objeto de Estudio</b>	<b>4</b>
<b>Campo de Acción</b>	<b>4</b>
<b>Planteamiento del problema</b>	<b>4</b>
<b>Preguntas de Investigación</b>	<b>5</b>
<b>Subpreguntas</b>	<b>5</b>
<b>Objetivos</b>	<b>6</b>
<b>Objetivo general</b>	<b>6</b>
<b>Objetivos específicos</b>	<b>6</b>
<b>Justificación</b>	<b>7</b>
<b>Marco Teórico</b>	<b>8</b>
<b>Marco conceptual</b>	<b>10</b>
<b>Marco Espacial</b>	<b>14</b>
<b>Marco Temporal</b>	<b>15</b>
<b>Aspectos Metodológicos</b>	<b>15</b>
<b>Métodos de Estudio</b>	<b>15</b>
<b>Preliminar Trabajo de Grado</b>	<b>17</b>
<b>Anexos</b>	<b>19</b>
<b>Bibliografía</b>	<b>20</b>

## **Título del Tema**

Evaluación de Riesgos y Controles para el uso de Tecnología Cloud Híbrida en GSI International.

### **1.1 Definición del objeto de estudio, del campo de acción y del modelo y/o instrumento del objeto de estudio en ese campo de acción.**

Se busca evaluar los riesgos y a la vez, establecer controles al momento de adquirir la Tecnología Cloud híbrida para la empresa GSI International, lo que se debe tomar en cuenta y lo que se debe hacer para llevar a cabo la migración de información hacia la nube, como manejar todo con el debido nivel de seguridad para mantener la integridad de los datos importantes de la antes mencionada empresa. De esta manera también se busca mejorar la inversión económica en la empresa, ya que la implementación de dicha tecnología tiende a mejorar todo lo que tiene que ver con los procesos en la empresa y aunque esto conlleva un precio, la relación beneficio-costos es mucho mejor que al no tenerla.

### **Objeto de Estudio**

Empresa GSI International

### **Modelo o Instrumento**

- Solución de sistemas en Bizagi
- Servidores Azure

## **Campo de Acción**

- Tecnología Híbrida Cloud

## **Planteamiento del problema**

Actualmente la empresa GIS International brinda servicios de automatización de procesos utilizando la herramienta Bizagi, que está basada en la notación y metodología BPMN 2.0. Dicha notación y el modelo de procesos comerciales se han convertido en el estándar para los diagramas de procesos comerciales. Está destinado a ser utilizado directamente por las partes interesadas que diseñan, administran y realizan procesos de negocios, pero al mismo tiempo son lo suficientemente precisos como para permitir que los diagramas BPMN se traduzcan en componentes de procesos de software. BPMN tiene una notación similar a un diagrama de flujo fácil de usar que es independiente de cualquier entorno de implementación particular.

Como mencionamos anteriormente la empresa GSI International está implementando sus proyectos con la herramienta llamada Bizagi. La misma es una suite ofimática con dos productos complementarios, un Modelador de Procesos y una Suite de BPM.

Bizagi Process Modeler es un Premium utilizado para diagramar, documentar y simular procesos usando la notación estándar BPMN (Business Process Modeling Notation).

Bizagi BPM Suite es una solución de Gestión de procesos de negocio (BPM) que les permite a las organizaciones ejecutar/automatizar procesos o flujos de trabajo (workflows).

En la actualidad la Empresa GSI International ha implementado soluciones de automatización de procesos en varias instituciones bancarias en República Dominicana. En los últimos años la empresa ha determinado que algunas pequeñas instituciones bancarias no cuentan con el presupuesto necesario para realizar la implementación de

un sistema que automatice algunos de sus principales procesos, esto debido a que automatizar desde cero conlleva una gran inversión. La empresa está proponiendo ante esta dificultad, implementar en una solución cloud algunos de los principales procesos de dichos bancos.

### **Preguntas de Investigación**

¿Existe actualmente una evaluación de los riesgos y controles para el uso de tecnología cloud híbrida en GSI International?

#### **Subpreguntas**

¿Es posible analizar los requerimientos y las necesidades actuales que pudiera haber para la evaluación y gestión del riesgo para la migración de los procesos establecidos a un sistema cloud?

¿Existe actualmente un modelo de evaluación de riesgos para la implementación de esta nueva tecnología?

¿Existe en la actualidad un protocolo o procedimiento de gestión de riesgo para cuando se implemente la tecnología cloud en la empresa?

### **Objetivos**

#### **Objetivo general:**

Evaluar los riesgos y controles para el uso de tecnología Cloud Híbrida en GSI International.

**Objetivos específicos:****Objetivo 1:**

Analizar los requerimientos y necesidades actuales para la evaluación y gestión del riesgo de la empresa para fines de migración a la tecnología Cloud Híbrida.

**Objetivo 2:**

Elaborar y diseñar un modelo de evaluación y gestión de riesgo para fines de la implementación de la nueva tecnología Cloud Híbrida.

**Objetivo 3:**

Determinar la forma en la que se implementaría el cambio a una tecnología cloud híbrida tomando en cuenta la gestión del riesgo tecnológico.

**Justificación**

Esta investigación es conveniente porque a partir de ella se puede determinar una propuesta acertada a la empresa GSI International para fines de la evaluación y gestión del riesgo tomando en cuenta la migración de procesos hacia una tecnología cloud híbrida, este paso traería consigo mayor posicionamiento a nivel de mercado y la expansión de la cartera de clientes.

Este tipo de tecnología tiene como objetivo simplificar y brindar opciones adicionales a pequeñas y medianas empresas del sector bancario para poder obtener servicios en las nubes de procesos automatizados y/o adaptados a su empresa con un menor costo, esto debido a que requeriría menos inversión de tiempo y de personal para desarrollo.

En la actualidad existen diferentes empresas internacionales de renombre que ofrecen este tipo de servicios y entre las principales ventajas que se encuentran en la tecnología cloud híbrida está el acceso desde cualquier dispositivo, actualización

constante de tecnología, pago por el uso de servicio de acuerdo a lo establecido, capacidad de almacenamiento ilimitada, disminución de uso de hardware, entre otros.

Otros de los beneficios que brinda esta tecnología es el servicio confiable, flexible y de alta escalabilidad.

La prioridad de desarrollar este tema es mejorar el catálogo de productos a ofrecer a los clientes y con esto poder brindar un mejor servicio mediante la aplicación de la tecnología Cloud Híbrida, esto produciría una mejora en el trabajo diario de cada uno de sus clientes, además se estaría posicionando a dicha empresa en un rango mayor ya que es importante mantenerse innovando y buscando mejores formas de hacer las cosas, tratando siempre de usar e implementar las últimas tecnologías disponibles.

### **Marco Teórico**

En la actualidad existen diferentes empresas a nivel internacional y nacional que brindan el tipo de tecnología de cloud para fines comerciales y por tanto existe amplia información en la red vinculada a este tema y a la gestión del riesgo tecnológico. Basado en esto tomaremos como referencia algunos de los más destacados para el desarrollo de nuestro tema.

Beltrán, M., y Sevillano, F. (2013) en su libro *“Cloud Computing, tecnología y negocios”* se proponen a estudiar el uso de la tecnología cloud en los negocios y su rápido crecimiento, así como las ventajas e inconvenientes de uso. Para realizaron un levantamiento de informaciones acerca de esta tecnología, así como referencias de otros autores que la han hecho uso de la misma. La conclusión a la que llegaron fue que la tecnología Cloud ha tenido aceptación por su flexibilidad y costo conveniente, también plantearon que los conceptos establecidos en su estudio pueden ser tomados como referencia actual de esta tecnología como para el futuro por personas inclusive que no manejen niveles muy técnicos de informática y se encuentren más orientados al área de negocios.

Vera-Rivera, F., y Pérez-Gutiérrez, B. (2016) en su investigación *“Modelo de Nube Híbrida (Hybrid Cloud) de infraestructura como servicio en el rendimiento de la plataforma SANDBOX - UFPS”* se proponen a estudiar el desarrollo de un modelo de nube híbrida de infraestructura como servicio con el fin de mejorar el rendimiento de la plataforma Sandbox de la Universidad Francisco de Paula Santander (UFPS). Para esto se basaron en el diagnóstico de la tecnología utilizada actual y luego realizaron un sondeo entre proveedores de computación en la nube existentes en el mercado. La conclusión a la que llegaron fue que con este cambio se mejora la disponibilidad, integridad y respaldo de la plataforma, siendo un referente para otras instituciones, empresas en general y para proveedores de infraestructura. Con este tipo de herramientas se automatiza el proceso de despliegue de aplicaciones y bases de datos y facilita el trabajo en equipo.

Rey-Arenas, N. (2017) en su investigación *“La contratación de servicios de cloud computing: movimientos internacionales de datos y gestión de riesgos de privacidad y seguridad”* Se propone a estudiar los diferentes movimientos internacionales de Datos y leyes aplicables al Cloud Computing. Para ello se sustentó en documentación e informaciones suplidas por los diferentes organismos de jurisdicción y otras directrices vinculadas al tema. La conclusión a la que llegó es que existen diferentes regulaciones para las informaciones compartidas en el internet a través de la tecnología cloud que, aunque se encuentran vigente pueden no garantizar cien por ciento la seguridad de la información si no se toman las medidas pertinentes.

Céspedes Leguizamón, C. (2016) en su investigación *“Servicios, Amenazas y Gestión del riesgo en la nube”* Se propone a estudiar la forma en la que la tecnología cloud pasó de ser una moda a una necesidad donde las compañías pequeñas pueden acceder a sistemas o tecnología utilizada por grandes empresas tomando en cuenta uso de normas de seguridad. Para ello se sustentó en normativas presentadas por ISACA donde se toman tres renglones principales para fines de gestionar adecuadamente el riesgo. La conclusión a la que llegó fue que existen diferentes recomendaciones a tomar

en cuenta para poder eficientizar la gestión de la nube tomando siempre en cuenta proteger la información de alto valor.

Estas fuentes de información citadas anteriormente serán de ayuda para sustentar de forma teórica y como referencia el estudio que estaremos llevando a cabo en lo adelante con los ejes principales de tecnología cloud, riesgo y las herramientas que intervienen en dicho proceso.

## **Marco Conceptual**

### **Generales Cloud Computing**

#### **1.1. Definición Cloud**

Hace referencia a un tipo de arquitectura informática que se define como “una tecnología que permite ofrecer servicios de computación a través de Internet” totalmente (online), básicamente en la nube (Cloud).

#### **1.2. Tipos de Tecnología Cloud**

Existen tres tipos de nubes:

- Nubes públicas, de uso mundial o global.
- Nubes privadas, son orientadas a soluciones corporativas.
- Nubes híbridas, son una mezcla de las dos nubes anteriores.

#### **1.3 Tecnología Cloud Híbrida**

Una nube híbrida es un entorno informático que combina una nube pública y una nube privada al permitir que se compartan datos y aplicaciones entre ellos. Cuando la demanda de computación y procesamiento tiene cambios, la computación en la nube híbrida brinda a las empresas la capacidad de escalar sin problemas su infraestructura local hasta la nube pública para manejar cualquier desbordamiento, sin dar a otros centros de datos acceso a la totalidad de sus datos.

### **1.3.1 Ventajas Tecnología Cloud Híbrida**

Las características más resaltantes de esta tecnología podrían resumirse en 4: escalabilidad, virtualización, ubicuidad y modelos de pago en función del uso. Ahorro de tiempo y ahorro de costes, y la mejora de la productividad de la empresa. Dicho ahorro de coste se traduce en ahorro de Colaboración, coste de mantenimiento, de coste de inversión, de coste de las licencias de software.

### **1.3.2 Desventajas Tecnología Cloud Híbrida**

Algunas desventajas o lo que más genera preocupación sería la seguridad, la confidencialidad, Pérdida de control de procesos, Dependencia del proveedor, dudas de disponibilidad, responsabilidad del proveedor, dificultad de migración y Costes variables no controlados. Estas son consideradas como las barreras a la hora de usar dicha tecnología: falta de conocimiento, las limitaciones presupuestarias, los costes elevados de contratación, la dificultad de migración, responsabilidad del proveedor, dudas de disponibilidad y dependencia del proveedor.

## **Conceptos de las Herramientas**

Business Process Model and Notation (BPMN), en español Modelo y Notación de Procesos de Negocio, es una notación gráfica estandarizada que permite el modelado

de procesos de negocio, en un formato de flujo de trabajo (workflow). BPMN fue inicialmente desarrollada por la organización Business Process Management Initiative (BPMI), y es actualmente mantenida por el Object Management Group (OMG), después de la fusión de las dos organizaciones en el año 2005.

## **2.2 BPM**

El BPM se puede definir como una nueva categoría de software empresarial que permite a las empresas modelar, implementar y ejecutar varias actividades interrelacionadas –es decir, Procesos– de cualquier naturaleza, ya sea dentro de un departamento o permeando la entidad en su conjunto, con extensiones para incluir a los clientes, proveedores y otros agentes como parte de las tareas en los procesos.

## **2.3 Bizagi**

BizAgi es la solución BPM que le permite a usted y a su organización diseñar, modelar, integrar, automatizar y monitorear sus procesos comerciales a través de un gráfico ambiente. Es la forma más rápida y eficiente de lograr la continua mejora de sus procesos.

## **2.4 Norma PCI/DSS**

El estándar de seguridad de tarjetas de pago PCI DSS ha tenido en los últimos años un auge derivado tanto de la gran cantidad de fraudes con tarjetas, como de la creciente presión regulatoria de las marcas de tarjetas sobre los comercios. Esta guía pretende, con un lenguaje sencillo y accesible, explicar desde el inicio los conceptos generales de PCI DSS de tal manera que el lector sea capaz de comprender su aplicabilidad, requisitos, cadena de supervisión y estrategia de implantación.

## **2.5 Capa SOAP**

Los servicios SOAP de Bizagi son uno de las dos APIs para acceso programático desde aplicaciones externas, como se describe en API de Bizagi.

Los métodos web de la Capa SOAP están agrupados dentro de las siguientes categorías, de acuerdo al servicio que representa un componente principal de la arquitectura de producto de Bizagi.

### **Gestión de Riesgo Tecnológico**

#### **3.1 Definición Evaluación**

Consiste en verificar un proceso o sistema para detectar y conocer las deficiencias y problemas que éste presenta.

#### **3.2 Riesgo**

El riesgo es una probabilidad de que ocurra un hecho que pueda ocasionar algún tipo de daño o pérdida. Esta palabra se relaciona mayormente con Peligro, Amenaza o Fuente de riesgo, y se usa para enfatizar el significado probabilístico.

#### **3.3 Riesgo Tecnológico**

El riesgo tecnológico es una vulnerabilidad que puede estar presente tanto en la infraestructura (hardware) como en la parte lógica o de sistemas, también es el uso inadecuado de dichos factores.

### **3.4 Evaluación de Riesgo Tecnológico**

La evaluación de riesgo es un elemento clave para la planificación de la acción preventiva en una empresa, puesto que a partir de ella se elaborarán y desarrollarán las medidas de protección y corrección que crearán unas condiciones de seguridad y salud adecuadas.

Para evaluar el riesgo tecnológico, debemos saber: si la tecnología utilizada está suficientemente controlada.

- si la vida del proyecto es o no sustancialmente superior al plazo de la financiación otorgada (concepto cola).
- si la planta o instalaciones producidas se han proyectado de manera que puedan seguir siendo competitivas a lo largo del tiempo.
- si existe disponibilidad de piezas y partes críticas para posibles eventualidades.

El caso de que las cuatro premisas anteriores tengan una respuesta afirmativa, las entidades financieras aceptaran el riesgo técnico.

### **3.5 Controles**

Consiste en una revisión periódica de un proceso, sistema, herramienta, etc. para fines de comprobar su correcto funcionamiento en relación a un objetivo pautado y de manera posterior realizar cualquier ajuste o corrección.

### **3.6 Amenaza**

Consiste en un posible riesgo, puede estar considerado en estas fallas en sistemas, accidentes, procedimientos, desastres naturales, etc. También se consideran como los factores externos que frenen el desarrollo de cualquier proceso.

### **Marco Espacial**

Este estudio va destinado a la Empresa GSI International, la misma está ubicada en el sector el vergel, del distrito nacional en la ciudad de santo domingo, República Dominicana.

### **Marco Temporal**

Esta investigación comprenderá del año 2019 al año 2020. Cabe mencionar que el proyecto que propone la empresa GSI International está ya en fase de construcción, por lo que se espera la solución esté terminada para el presente año 2020. El tiempo estimado para finalizar este proyecto es de 6 meses.

### **Aspectos Metodológicos**

#### **Tipo de estudio:**

Los aspectos metodológicos en este trabajo final son:

#### **Descriptivo**

La investigación será descriptiva ya que nos basaremos en estudiar el proceso actual, en observar cómo funciona y al mismo tiempo describir sus características para

tener un enfoque exacto para el estudio que estaremos realizando. Haremos uso a su vez de una encuesta para recopilar información útil por parte de los clientes y usuarios.

### **Exploratorio**

La investigación se fundamentó en explorar el tema y en encontrar posibles soluciones para fines de llevar el proceso pautado durante el proceso de investigación, para esto se estarán formulando preguntas que serán desarrolladas a lo largo de la misma.

### **Métodos de Estudio**

#### **Analítico**

Esto debido a que nuestro tipo de investigación estará orientada a observar cada uno de los subprocesos y ver su funcionamiento con el fin de conocer la naturaleza del objeto de estudio.

#### **Lógico deductivo**

Estaremos utilizando este tipo de método debido a que tomaremos principios generales que serán aplicados a un caso particular dentro del objeto de estudio donde se podrían encontrar consecuencias desconocidas a partir de generalidades.

## **Esquema Preliminar del contenido del Trabajo de Grado**

**DEDICATORIAS**

**AGRADECIMIENTOS**

**RESUMEN**

**INTRODUCCIÓN**

**CAPÍTULO I. ASPECTOS GENERALES**

**1.1 Marco Legal**

**1.2 Concepto**

**1.3 Historia**

**CAPÍTULO II. TECNOLOGÍA CLOUD**

**2.1 Conceptos**

**2.2 Clasificación y características**

**2.3 Requerimientos**

**2.4 Ventajas y desventajas**

**CAPÍTULO III. EVALUACIÓN Y GESTIÓN DEL RIESGO TECNOLÓGICO**

**3.1 Conceptos**

**3.2 Características**

**3.3 Seguridad**

**3.4 Riesgo tecnológico orientado a servicios Cloud**

**3.5 Herramientas para seguridad**

**3.6 Integración con otros servicios**

## **CAPÍTULO IV. HERRAMIENTAS Y SOLUCIONES PARA NEGOCIOS**

### **4.1 Conceptos**

### **4.2 Herramientas principales**

### **4.3 Características**

### **4.3 Ventajas y desventajas de las diferentes herramientas**

## **CAPÍTULO V. SISTEMA**

### **5.1 Software**

### **5.2 Base de Datos**

### **5.3 Servidores**

## **CAPÍTULO VI.**

## **CAPÍTULO VI. METODOLOGÍA**

### **6.1 Tipos de Investigación**

### **6.2 Métodos**

### **6.3 Técnicas e Instrumentos**

## **CONCLUSIÓN**

## **RECOMENDACIONES**

## **BIBLIOGRAFÍA**

## **Anexos**

## Bibliografía

Object Management Group, Inc. (1997-2020). *Object Management Group Business Process Model and Notation*. Object Management Group. Recuperado de <http://www.bpmn.org/>

Beltrán, M. Sevillano, F. (Enero 1, 2013). *Cloud Computing, Tecnología y Negocio*. Ediciones Paraninfo, S.A. Recuperado de <https://books.google.com.do>

Vera-Rivera, F, H. Perez-Gutierrez, B, R. Urbina, V, M. (2016). *MODELO DE NUBE HÍBRIDA (HYBRID CLOUD) DE INFRAESTRUCTURA COMO SERVICIO PARA MEJORAR EL RENDIMIENTO DE LA PLATAFORMA SANDBOX - UFPS*. Conferências Ibero-Americanas WWW/Internet e Computação Aplicada. Recuperado de <https://www.researchgate.net>

Céspedes, C, A. (s.f). *SERVICIOS, AMENAZAS Y GESTIÓN DEL RIESGO EN LA NUBE*. Universidad Piloto de Colombia. Recuperado de <http://polux.unipiloto.edu.co>

EcuRed. (s.f). *Tecnología de Nube*. EcuRed. Recuperado de <https://www.ecured.cu>

Microsoft. (2020). *¿Qué es una nube híbrida?*. Microsoft Azure. Recuperado de <https://azure.microsoft.com>

Zabala-Vivanco, J. Rio-Belver, R. Cilleruelo-Carrasco, E. Garechana-Anacabe, G. Gavilanes-Trapote, J. (Junio, 2013). *Beneficios del Cloud Computing para la Pequeña y Mediana Empresa*. Technology Foresight Management (TFM). Recuperado de <https://www.researchgate.net>

Auraportal. (Anexo I. Anteproyecto 2020). *¿Qué es BPM?*. Miami, E.U.: Auraportal. Recuperado de <https://www.auraportal.com>

Goetz, M. (s.f). *Modeling Workflow Patterns through a Control-flow perspective using BPMN and the BPM Modeler BizAgi*. Institute of Applied Informatics and Formal Description Methods University Karlsruhe (TH). Recuperado de <http://wiki.recife.pe.gov.br>

Ferrini-Fonseca, D. (2019). *PCI Dss, Breve Guía Para El Cumplimiento*. Publicado Independientemente. Recuperado de <https://books.google.com.do>

## **ANEXO II- Modelo de Cuestionario para implementación de verticales**

¿Cómo calificaría su institución (Grande, Mediana, ¿Pequeña)?

¿Conoce usted la Notación BPMN?

¿Conoce o ha escuchado sobre Bizagi?

¿Ha escuchado sobre las soluciones en las nubes?

¿Cuenta usted en la actualidad con un sistema para gestionar las solicitudes de tarjetas de crédito y préstamos?

¿En caso de que su respuesta sea No, está dispuesto a adquirir un sistema automatizado para esta gestión?

¿En caso de que su respuesta a la pregunta 2 sea Si, le gustaría una aplicación que le ayudará a optimizar este proceso integrándose con los sistemas actuales?

¿Le interesaría tener una aplicación de esta magnitud en las nubes?

¿Le interesaría tener acceso a esta aplicación desde su teléfono móvil?

¿Qué cantidad de tiempo aproximado en horas dura una solicitud en sus sistemas actuales?

¿Entiende usted que los procesos actuales pueden ser optimizados con una solución en las nubes bajo la notación de BPMN?

¿Estaría dispuesto(a) a recibir una prueba de concepto de estas verticales para ver el valor que le aportaría a su empresa?