Decanato de Ingeniería e Informática
Escuela de Informática

"Análisis para la Implementación de un Modelo de Continuidad de Negocio y Recuperación de Desastres Basada en la Nube para la EMPRESA REYES & HERMANOS", Santo Domingo R.D. 2014"

Sustentantes:

Francis Subervi	**1998-2222**
Eduardo Pérez	**2007-2391**
Julio Reyes	**2001-0227**

Asesor:
Ingeniero Santo Navarro

Monografía para Optar por el Título de:
Ingeniero en Sistemas

Distrito Nacional, República Dominicana
2014

Análisis para la Implementación de un Modelo de Continuidad de Negocios y Recuperación de Desastres Basada en la Nube para la EMPRESA REYES & HERMANOS", Santo Domingo R.D. 2014

DEDICATORIAS

A mi esposa Lisbeth Ortiz, por soportar las horas de ausencia y por animarme a completar este ciclo en mi vida académica. Mi triunfo te lo dedico especialmente a Ti. A mis padres Julio Reyes y Carmen León, por su apoyo, su amor, sus consejos y sus enseñanzas durante toda mi vida. A mis hermanas, Magnolia Reyes y Sabrina Reyes que han sido uno de mis principales apoyos y quienes siempre han estado presentes en mis victorias y mis derrotas.

Y a todos aquellos amigos, familiares y compañeros de labores que han estado al pendiente de mi desarrollo y formación personal en especial: Federico Muller y Jonatán Espinosa.

Julio Reyes

DEDICATORIAS

Con todo mi cariño y mi amor para las personas que hicieron todo en la vida para que yo pudiera lograr mis sueños, por motivarme y darme la mano cuando sentía que el camino se terminaba, a ustedes por siempre mi corazón y mi agradecimiento. Mi padre Juan Carlos Subervi, Mi madre María Altagracia Escarramán, Mi esposa Claudia Patricia Rojas Ramírez.

Francis Subervi

DEDICATORIAS

Gracias a esas personas importantes en mi vida, que siempre estuvieron listas para brindarme toda su ayuda y apoyo, ahora me toca regresar un poquito de todo lo inmenso que me han otorgado. A mis padres, mis hermanas, tíos, abuela y demás familiares, también a mis amigos con todo mi cariño está tesis se las dedico a ustedes.

Eduardo Pérez

AGRADECIMIENTOS

A Dios todopoderoso quien es que él pone el querer y el hacer.

A nuestro asesor Ing. Santo Navarro, por brindarnos sus conocimientos y trazarnos las pautas para realizar un excelente proyecto.

A los profesores que a lo largo de la carrera nos han traspasado muchos de sus conocimientos y experiencias para que hoy podamos ser los profesionales que somos en especial a: Ramón Gómez, Hipólito Tavera y Víctor Herrera.

A mis compañeros Francis Subervi y Eduardo Pérez, por todo el esfuerzo, malas noches y trabajo para llevar adelante este proyecto. A mis amigos y compañeros especialmente amigos como Wilson Ramírez, Anderson Veras, por su gran apoyo e increíbles consejos.

Julio Reyes

AGRADECIMIENTOS

El presente trabajo de grado es un esfuerzo, en el cual, directa o indirectamente, participaron varias personas leyendo, opinando, corrigiendo, teniéndome paciencia, dando ánimo, acompañando en los momentos de crisis y en los momentos de felicidad. Agradezco a los profesores Santo Navarro y Ramón Gómez por haber confiado en mi persona, por la paciencia y por la dirección de este trabajo.

Gracias también a mis queridos compañeros, que me apoyaron y me permitieron entrar en su vida durante estos casi cuatro meses de conviví dentro y fuera del salón de clase. Julio Reyes, Eduardo Pérez.

A mi madre y a mi padre que me acompañaron en este trabajo de gradoy que de forma incondicional, entendieron mis ausencias y mis malos momentos.

Francis Subervi

AGRADECIMIENTOS

Antes que nada quiero encomendar este logro en mano de Dios, ya que él es el responsable de que pueda alcanzar esta etapa en mi vida y de bendecirme siempre para que no pierda las fuerzas. Gracias al apoyo y oraciones de mi madre Maritza Mercedes, una mujer incondicional que siempre ha estado ahí para mí. Gracias a mi padre Eduardo Rosario un ejemplo de honestidad y seriedad que nunca me dijo que no cuando necesité de su ayuda.

A la institución experiencia dominicana que por medio de la escuela la Salle pude obtener una beca la cual me ayudó a costear la gran parte de mis gastos universitarios.

Agradecer a mis hermanas, míos tíos, mi abuela y demás familiares y amigos, que de una manera u otra aportaron su granito de arena a este propósito y de que yo pueda hacer de un sueño una realidad.

También agradecer a los profesores que fueron mi guía, al Ing. Santos Navarro mi asesor de monográfico y a los compañeros de universidad que estuvieron conmigo en este gran proyecto, Francis Subervi y Julio Reyes.

Eduardo Pérez

INDICE

INDICE GRAFICOS

INDICE TABLAS

INTRODUCCION

En esta investigación se pretende integrar tecnología de punta, específicamente computación en la nube (Cloud Computing), para la EMPRESA REYES & HERMANOS, con el fin de, garantizar la continuidad de sus operaciones y de los servicios que ofrece, tanto a sus clientes internos como externos. La computación en la nube es un sistema basado en internet y de centros de datos remotos, la cual involucran la integración de varios servicios. La seguridad de la información y el sistema de continuidad de negocios juegan un papel importante al momento de evaluar cualquier proveedor de estos servicios, uno de los factores críticos que son evaluados por las empresas es la capacidad de tener sus servicios disponibles ante cualquier evento, los acuerdos de nivel deservicios, la gobernabilidad y gestión de la información, regulaciones y cumplimiento de políticas, son temas a discutir durante el proceso de la evaluación del contrato de servicios en la nube (Cloud Computing).

Bajo este mismo esquema se creara un plan de continuidad de negocios que le permita a la EMPRESA REYES & HERMANOS responder ante cualquier falla o desastre basado en las mejores prácticas y regulaciones de la industria. Esto incrementara la capacidad de acceso a los servicios para apoyar la toma de decisiones. Los planes de recuperación y el análisis de impacto son elementos a tomar en cuenta, al momento de realizar una implementación de continuidad de negocios integrada con la infraestructura actual de una empresa.

PLANTEAMIENTO DEL PROBLEMA

En un estudio realizado por la empresa consultora global continuity, se llegó a la conclusión de que las pérdidas financieras asociadas a las Interrupciones de servicio Tecnología de la Información (TI) se disparan cuanto más tiempo tardan en resolverse.

Según “The Avoidable Cost of Downtime” los departamentos más afectados por el tiempo de inactividad son las operaciones (62%), finanzas (48%) y adquisiciones (39%), para Estados Unidos. Recuperado http://www.audisec.es/docs/continuity/fichaglobalcontinuity.pdf

Para el caso de Europa el informe ‘Avoidable Cost of Downtime 2010’, realizado por la firma de investigación independiente Coleman Parkes a petición de CA Technologies, estima que las pérdidas financieras asociadas a las interrupciones de servicio Tecnología de la Información (TI) y al tiempo que tardan en recuperarlo, alcanzan los 3,000 millones.

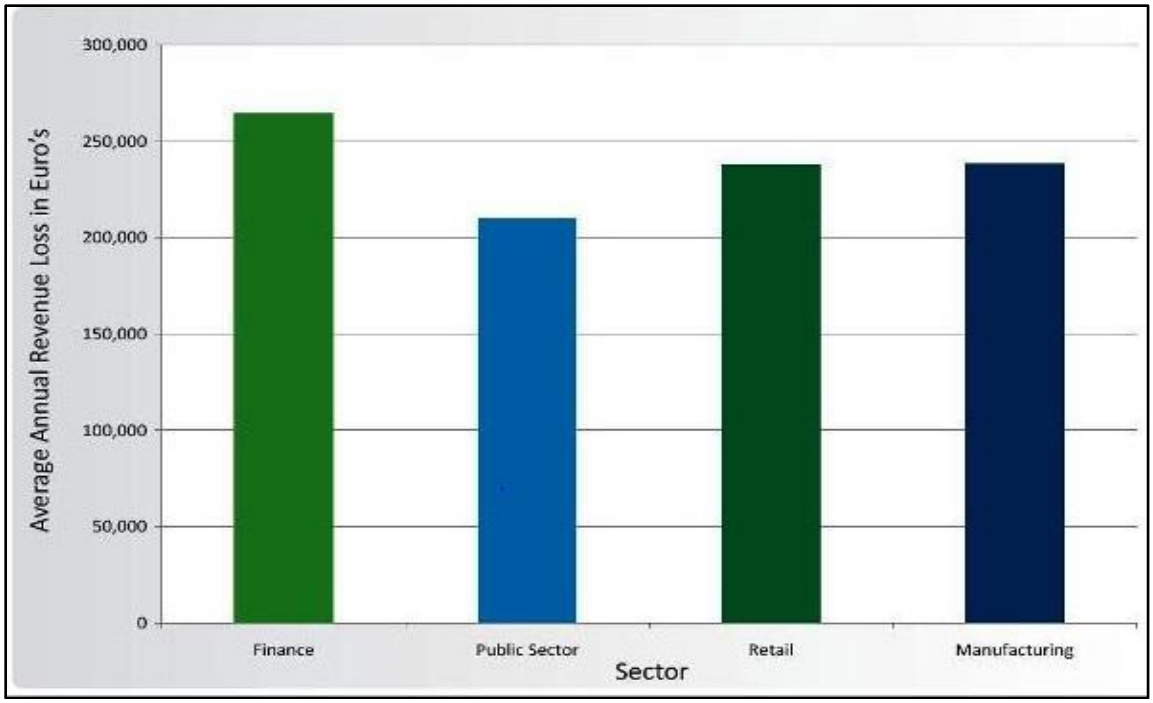


Grafico 1. El costo evitable de tempo de inactividadFuente propia basada en el reporte de Computer Associate theimpact of IT downtime on employee productivity

Los resultados de este estudio evidencian también que cada firma española registra una media de diez horas de interrupción del servicio Tecnología de la Información (TI) al año, esto es más de 90.000 horas en el conjunto de España. Y cuando los sistemas Información importantes no funcionan, las organizaciones estiman que su capacidad para generar ingresos queda reducida a un 36%. Los departamentos que más se ven afectados por estas interrupciones son los de Operaciones (62%), Ventas (52%) y Finanzas (52%).

La EMPRESA REYES & HERMANOS no cuenta con un emplazamiento en la nube para planificación de continuidad del negocios (BC) y recuperación ante desastres (DR) que aborde incidentes como cortes de corriente, incendios,

inundaciones, huracanes, terremotos, tornados e incluso robo, esto afecta la productividad del negocio e imagen de la empresa. Tener una solución de continuidad de negocio propietario involucra altos costo de infraestructura tecnológica, regulaciones, cumplimiento de estándares y personal altamente calificado para la gestión técnica.

Por otro lado, se suma la responsabilidad de la seguridad de la información y el almacenamiento de grandes volúmenes de información.

Recuperado:http://www.computing.es/infraestructuras/tendencias/1034402001801/coste-interrupciones-servicio-espana.1.html:

OBJETIVOS DE LA INVESTIGACION

Objetivo General

Optimización de la operación tecnológica para asegurar la continuidad de los procesos, logrando una reducción de costos por fallas, mediante un esquema de continuidad de negocios y recuperación de desastres basado en la nube.

Objetivos Específicos

- Mejorar la operación tecnológica, bajo un enfoque de continuidad de negocios y recuperación de desastres basado en la nube.
- Crear un plan de contingencia operativa que permita la recuperación y continuidad de la empresa frente a fallas y/o desastres basada en un estándar de recuperación de desastres.
- Incrementar la capacidad de acceso a los servicios para apoyar la toma de decisiones.
- Disminución de costo ocasionado por fallas y/o desastres naturales o tecnológicos.
- Incrementar los niveles de satisfacción de clientes internos y externos, a través de la disponibilidad de los procesos.
- Identificar las necesidades de continuidad de servicios.

CAPITULO I.
INFORMACIÓN ORGANIZACIONAL

1.1 ¿Quiénes somos?

Reyes & Hermanos una empresa manufacturera que se dedica a la fabricación y distribución de productos de consumo masivo.

Actualmente estamos ocupando los primeros lugares del mercado con base en el desarrollo de productos innovadores que pretenden satisfacer el gusto del consumidor de la República Dominicana.

1.2 Misión

Desarrollar productos innovadores y diferentes que satisfagan los gustos y necesidades del consumidor Dominicano, posicionándonos como una empresa líder en las áreas donde compite.

1.3 Visión

Ser reconocidos en República Dominicana como una compañía de éxito, que cambia las áreas donde competimos. Solidificaremos la presencia de nuestras marcas e incursionaremos en nuevas categorías, ofreciendo a nuestro público calidad e innovación.

1.4 Objetivos

Nuestros éxitos y principios, servirán de guía e inspiración para toda la gente que nos rodea influyendo en los mismos para que transformen paradigmas y se convenzan que con pasión, determinación y autodisciplina, no hay imposibles.

1.5 Valores

- **Respeto:** Reconocer los derechos y la dignidad de las personas.

- **Transparencia:** Generar confianza y manejar con claridad las relaciones tanto de clientes internos como de externos.

- **Honestidad:** Actuar de acuerdo con los principios y convicciones que predica la organización, congruencia entre lo que se dice y lo que se hace.

- **Justicia:** Atribuir a cada persona aquello que ha logrado, aquello a lo que tiene derecho.

- **Responsabilidad:** Asumir las consecuencias de los actos y cumplir con las obligaciones.

1.6 Estructura Organizacional

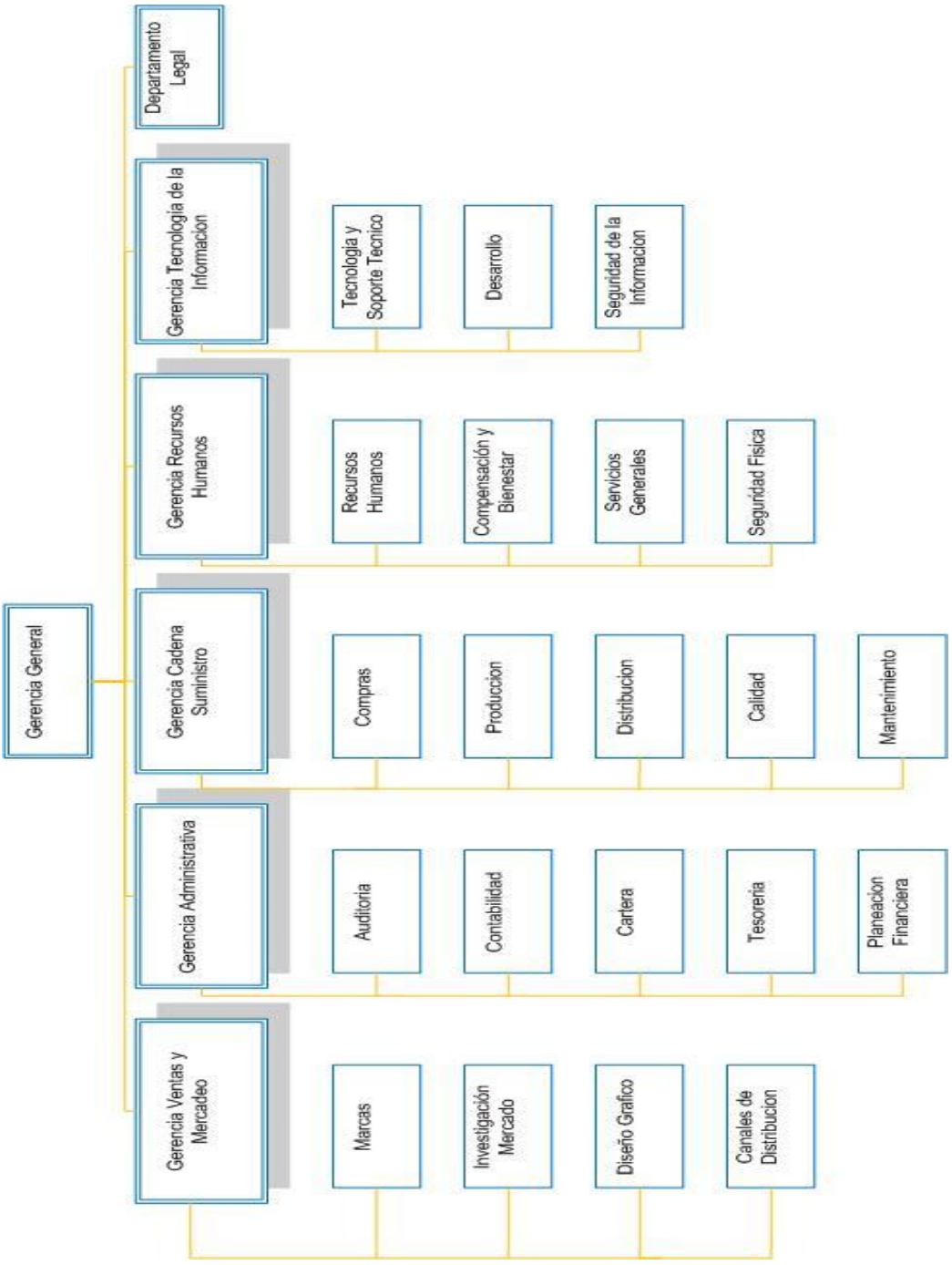


Grafico 2. Estructura Organizacional EMPRESA REYES & HERMANOS. Fuente propia.

1.7 Productos

La EMPRESA REYES & HERMANOS fabrica distribuye y vende una diversidad de productos naturales, tales como:

- Suplementos Alimenticios “El Natural”
- Pan Integral “El Natural”
- Galletas de Trigo “El Natural”
- Energizarte a Base de Ginseng “El Natural”
- Omega 3 “El Natural”

CAPITULO II.
CONCEPTOS GENERALES

En este capítulo se presentan los conceptos generales de la investigación sobre la Computación en la Nube, así como todo lo relacionado con la seguridad, aspectos legales, riesgo y cumplimientos y gobernabilidad y gestión.

2.1 Computación en la Nube

Es un modelo que permite el acceso bajo demanda y a través de la red a un conjunto de recursos compartidos y configurables (Como redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser rápidamente asignados y liberados con una mínima gestión por parte del proveedor del servicio. Según el Instituto Nacional de Estándares y Tecnología, siglas en inglés (NIST) la nube de cumplir con las siguientes características:

- **Autoservicio Bajo Demanda:** El usuario puede acceder a capacidades de computación en la nube de forma automática según requiriendo sin necesidad de una interacción humana con su proveedor o sus proveedores de servicio.

- **Múltiples Formas de Acceder a la Red:** Los recursos son accesibles a través de la red y por medio de mecanismos y estándares que son utilizados por una amplia variedad de dispositivos de usuarios, desde teléfonos móviles a ordenadores portátiles o Asistente Digital Personal, siglas en inglés (PDA).

- **Compartición de Recursos:** Los recursos (Almacenamiento, memoria, ancho de banda, capacidad de procesamiento, máquinas virtuales, etc.) de los proveedores son compartidos por múltiples usuarios, a los que se van asignando capacidades de forma dinámica según sus peticiones, los usuarios pueden ignorar el origen y la ubicación de los recursos a los que acceden, aunque si es posible que sean conscientes de su situación a determinado nivel, como el del centro de procesamiento de datos.

- **Elasticidad:** Los recursos se asignan y se liberan rápidamente, muchas veces de forma automática, lo que les da a los usuarios la impresión de que los recursos a su alcance son ilimitados y están siempre disponibles.

- **Servicio Medio:** El proveedor es capaz de medir, a determinado nivel, el servicio efectivamente entregado a cada usuario, de forma que tanto proveedor como usuario tienen acceso transparente al consumo real de los recursos, los que posibilita el pago por el uso efectivo de los servicios.

Las tecnologías de Computación en la Nube ofrecen tres modelos de servicio:

- **Programa como Servicio (Cloud Software as a Service):** En este modelo se ofrece la capacidad de que las aplicaciones que su proveedor le suministre corran en una infraestructura, siendo las aplicaciones accesibles a través de internet.

- **Plataforma como Servicio (Cloud Platform as a Service):** Permite desplegar aplicaciones propias (ya sean adquiridas o desarrolladas por el propio usuario) en la infraestructura nube de su proveedor, que es quien ofrece la plataforma desarrollo y las herramientas de programación. En este caso, el usuario es quien mantiene el control de la aplicación, aunque no de toda la infraestructura subyacente.

- **Infraestructura como Servicio (Cloud Infraestructura as a Service):** En este caso el proveedor ofrece al usuario recursos como capacidad de procesamiento, almacenamiento y comunicaciones que el usuario puede utilizar para ejecutar cualquier tipo de software, desde sistemas operativos hasta aplicaciones.

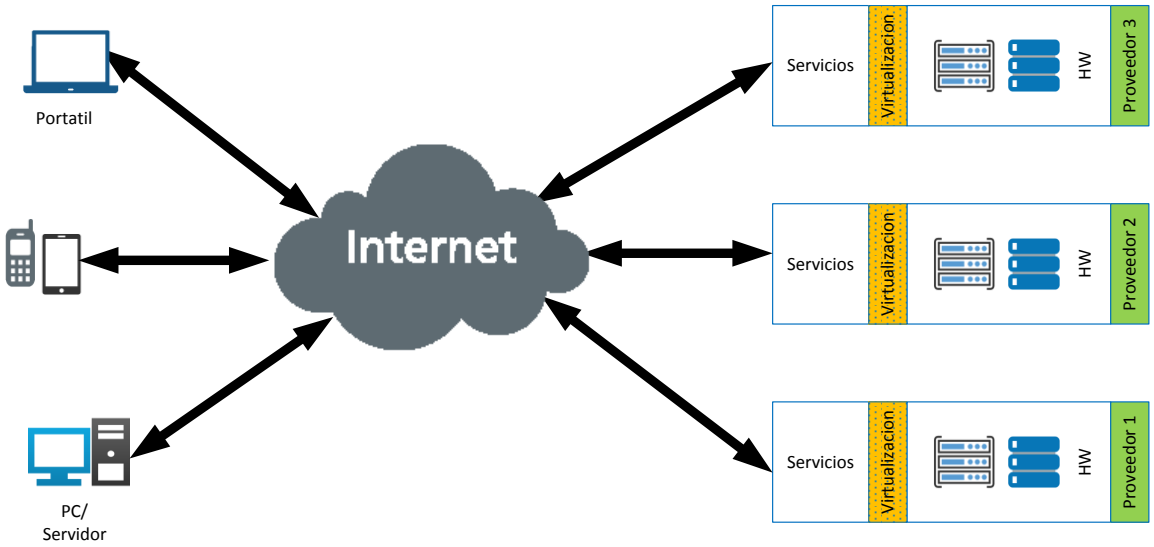


Grafico 3. Concepto de Computación en la Nube. Fuente propia basada en el libro Cloud Computing, Tecnología y Negocio.

Según el Instituto Nacional de Estándares y Tecnología, siglas en inglés (NIST), existen 4 formas de desplegar y operar una infraestructura de computación en la nube:

- **Nube Propia:** La infraestructura es íntegramente gestionada por una organización.
- **Nube Compartida:** La infraestructura es compartida por varias organizaciones.
- **Nube Pública:** La infraestructura es operada por un proveedor que ofrece servicios al público en general.
- **Nube Hibrida:** Es la combinación de dos o más nubes individuales que, pudiendo ser u su vez propias, compartidas o públicas, permite portardatos o aplicaciones.

Tecnologías de Cloud Computing

Es importante reconocer que los servicios en la nube no son siempre utilizados con la tecnología de virtualización. No existe un requerimiento o algún proceso para la abstracción de los recursos de los contenedores virtualizados.

Con lo que sabemos hasta ahora de este nuevo modelo de computación y de negocio, parece fácil comprender que, por un lado, es necesario disponer de tecnología como el Grid, que soporte las necesidades de recursos de hardware que presenta, pero por otro lado, también son necesarias tecnologías a un nivel de abstracción más alto que permitan ofrecer estos recursos a los usuarios con

las características mencionadas en la sección anterior. En concreto, estas tecnologías son las virtualización y los servicios Web, que resuelven la necesidad de ofrecer hardware y software de distintos tipos siguiendo unos estándares, a través de la red, con la prioridad de multi-tenencia (multi-tenacy) o compartición por parte de varios usuarios y manteniendo siempre la transparencia deseada.

- **Sistema Grid**

Las arquitecturas de tipo grid surgieron como la evaluación natural de los cluster, generalizando el concepto gracias a la gran evolución de internet. Aunque ambos tipos de arquitectura son de memoria distribuida, es decir, cada uno de los nodos que componen el sistema tiene su propia memoria principal que es accesible para el resto de los nodos, por lo que, la colaboración y comunicación entre ellos debe realizarse de manera explícita mediante paso de mensajes.

En el caso de un clúster, los nodos están ubicados geográficamente en el mismo lugar y se conectan entre ellos mediante un área controlada de altas prestaciones.

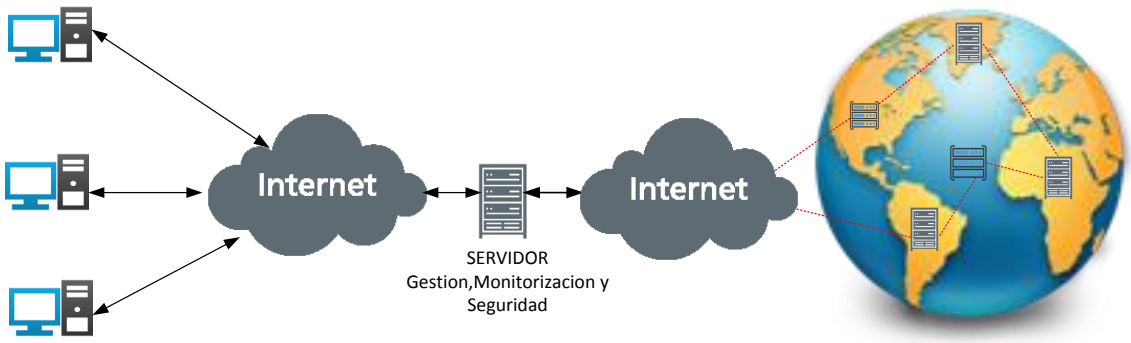


Grafico 4. Esquema de Arquitectura Grid. Fuente propia basada en el libro Cloud Computing, Tecnología y Negocio

- **Virtualización**

La virtualización consiste en utilizar los recursos de hardware y software de un equipo y multiplexarlos con el fin de crear varios equipos el cual funcionan de manera independiente utilizando los mismos recursos del equipo físico, es importante destacar que para aprovechar los recursos de la virtualización y realizar ciertas funciones avanzadas el equipo físico debe estar optimizado para estos fines, sin olvidarnos que la función de virtualización es realmente hecha por el software.

Esta técnica no es una tecnología nueva se conoce desde hace más de 30 – 40 años y los pioneros de esta tecnología fue IBM.

Francis Subervi, 2014

Según la empresa VMWARE pionera en las técnicas de virtualización lo definen como un contenedor de software muy aislado con un sistema operativo y aplicaciones. Debido a que, las máquinas virtuales son independientes y están

totalmente separadas, muchas de ellas se pueden ejecutar simultáneamente en una sola computadora. Una capa ligera de software llamada hipervisor desacopla las máquinas virtuales del anfitrión y asigna de manera dinámica recursos de computación a cada máquina virtual en la medida necesaria.

Se puede tener acceso a escritorios virtualizados, servidores virtualizados, almacenamiento virtualizado, sistemas operativos virtualizados o recursos de red virtualizados.

Todos estos recursos virtualizados se pueden utilizar con tanta efectividad como los recursos físicos para ejecutar operaciones comerciales.

Se pueden distinguir varios tipos de virtualización en función de la capa que se abstraiga, quizás una de las más conocidas sea la virtualización de software (o de la maquina).

En estos casos se utiliza un software para crear una máquina virtual que emule servicios y capacidades del hardware subyacente (Procesamiento, memoria, almacenamiento, comunicaciones).

Esto permite ejecutar más un sistema operativo en un único equipos físico sin necesidad de tener diferentes particiones.

En el caso del computación en la nube (cloud computing) la virtualización de maquina permite que los proveedores ofrezcan una infraestructura sin localización a sus clientes, de manera que para ellos la ubicación real de sus recursos sea completamente transparentes, y permite también que varias máquinas virtuales asociadas a diferentes usuarios , compartan recursos hardware en único equipo físico, el resto de tipos de virtualización (almacenamiento, red, etc.) completan en muchos casos a esta , que es la más básica pero también la imprescindible , ya que, se necesita para independizar las aplicaciones distribuidas de los recursos hardware y conseguir el dinamismo y la flexibilidad .

La virtualización de maquina se basa siempre en un hipervisor o monitor de máquina virtual, que hace de intermediario entre el hardware de la maquina real (Host) y el sistema operativo invitado (guest) instalado sobre la máquina virtual.

Es decir, que permita los accesos de este sistema operativo, guest al procesador, la memoria, los dispositivos de entrada y salida, el almacenamiento y la red.

Según una encuesta patrocinada por VMWARE, la mayoría de los encuestados (70 %) utilizaron la virtualización cuando resultó necesaria una actualización de hardware de grandes proporciones para evitar el costo que implicaba la compra de una gran cantidad de máquinas físicas. Aun así, una gran cantidad (52 %)

utilizaron la virtualización cuando resultó necesaria una migración importante de sistema operativo, por ejemplo de Windows XP a Windows 7. Además, el 51 % virtualizaron sus servidores cuando resultó necesaria una renovación importante de licencia de aplicaciones, como Oracle o SAP, y notaron que podían ahorrar de manera significativa por medio de la consolidación de servidores.

El mismo estudio arrojo que El 79 % de las empresas que ya han virtualizado experimentan ventajas “significativas”. Durante los próximos dos años, estas empresas planean invertir el 23 % de sus presupuestos de Tecnología de la Información (TI) en virtualización y convertir otro 32 % de los servidores en anfitriones virtuales.

Otras de las encuestas de VMWARE indican la continuidad del negocio es una de las inquietudes principales de las empresas que adoptan un entorno de Tecnología de la Información (TI) virtualizado. El 66 % de las empresas encuestadas establecieron que experimentaron una mejora en la continuidad del negocio tras implementar la virtualización.

Es probable que obtenga una o más de cuatro ventajas claves al virtualizar su entorno de Tecnología de la Información (TI):

- Mejora en la continuidad del negocio
- Simplificación de la administración de Tecnología de la Información (TI)

- Capacidad de reasignar recursos de Tecnología de la Información (TI) a fines más estratégicos
- Mejora en la capacidad de respuesta del negocio

Según el estudio realizado por VMWARE indica en la siguiente grafica el porcentaje de las mejoras que pudieron obtener utilizando la tecnología de virtualización, es importante destacar que este estudio fue patrocinado por VMWARE a empresas con menos de 1000 empleados.

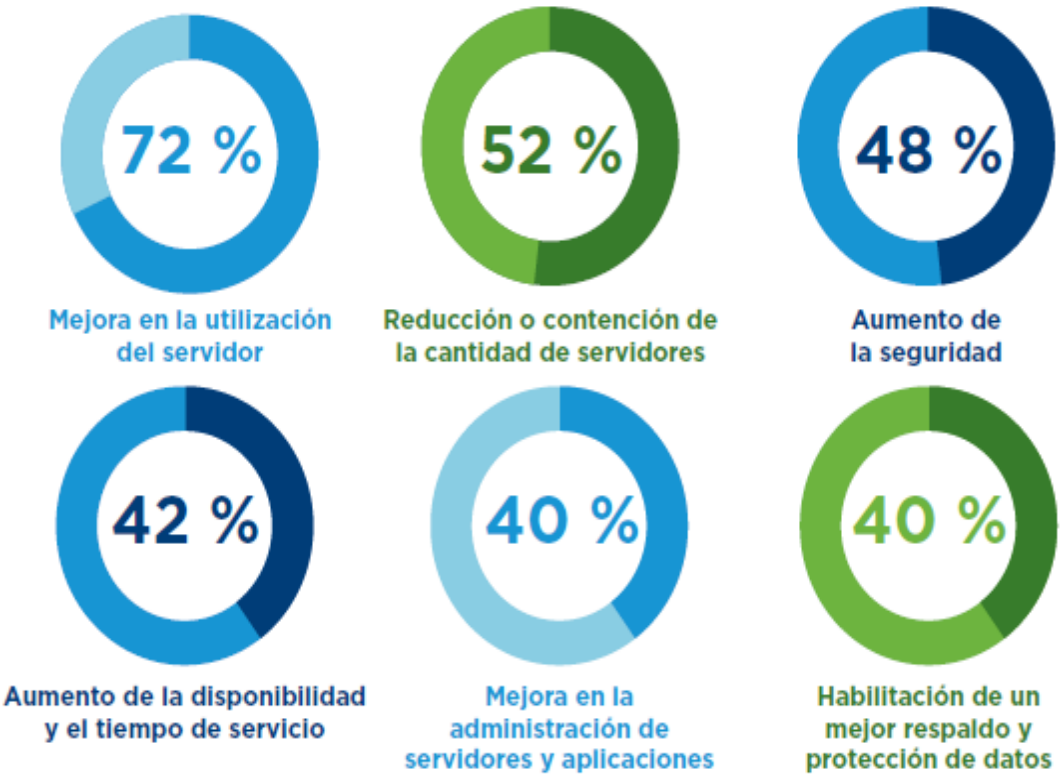


Grafico 5. Cuatro razones convincentes para virtualizar su entorno de Tecnología de la Información (TI). Fuente VMWARE.

Aspectos Legales Relacionados con la Computación en la Nube

- **Ley Orgánica de Protección de Datos de Carácter Personal de España (LOPD)**
  - Aspectos legales LOPD (I)
    - Supuesto: La puesta disposición de la información al Proveedor de servicios constituye un tratamiento de datos por un tercero, lo que puede dar lugar a una sesión incontenida de datos.
    - Soluciones Jurídicas: Redacción de un contrato encargado de tratamiento con el proveedor que regule el tratamiento de datos.
  - Aspectos legales LOPD (II)
    - Supuesto: La deslocalización de los servicios puede dar lugar a transferencias internacionales de datos, no autorizadas:
      - Si se traslada la información a servidores ubicados en el extranjero.
      - Si se produce acceso a la información desde un país extranjero.
    - Soluciones jurídicas:
      - Posibilidad de transferencia a países con nivel de protección adecuado.
      - Formalizar el contrato para la realización de transferencias internacionales de datos.

- Aspectos legales LOPD (III)
    - Supuesto: Las gestión de servicios en la nube provoca que el usuario pierda el control sobre la gestión de seguridad siendo necesario la implantación por proveedor y por el usuario de las medidas dirigidas a proteger la integridad y confidencialidad de los datos de la información.

    - Soluciones Jurídicas:
        - Garantía de la implantación de las medidas de seguridad por proveedor a nivel contractual.
        - Redacción del documento de seguridad en función de los compromisos adquiridos en el contrato por cada parte.
        - Recomendable que acredite certificaciones de cumplimiento de normativa (ISO).

- Aspectos legales LOPD (IV)
    - Control de acceso: El carácter multi-tenancy de los servicios a través de la nube provoca que varios usuarios estén utilizando los mismo recursos de un modo simultaneo lo que puede dar lugar a que se produzcan accesos no autorizados a la información.

- Soluciones Jurídicas:
  - Regular en el contrato de encargado de tratamiento la obligatoriedad de compartimentalizar la información al objeto de evitar que se mezcle con las de otros usuarios.
  - Inclusión de las medidas correspondientes en el documento de seguridad.

- Aspectos legales LOPD (V)
  - Supuesto: El usuario está obligado por la ley a realizar copias de seguridad de determinada información al objeto de impedir su pérdida. En la medida en que dicha información está gestionada a través de la nube se pierde el control por parte del usuario respecto de la ejecución de la misma.

  - Soluciones Jurídicas:
    - Necesario regular en el contrato de encargado de tratamiento a quién corresponde la obligación de llevar a cabo las mismas.
    - Inclusión el documento de seguridad dicha obligación en función de los compromisos adquiridos por las partes.

- Aspectos legales LOPD (VI)
  - La pérdida de la gestión de control de los sistemas de información por parte del usuario dificultan el conocimiento de

aquellas quiebras de seguridad que pudiesen producirse en las infraestructuras del proveedor.

- Soluciones Jurídicas:
  - Regulación por vía contractual de los mecanismos para la notificación de incidencias por parte del proveedor al usuario, así como la redacción de un protocolo para la gestión de las mismas.
  - Inclusión del procedimiento en el documento de seguridad de proveedor.

- Aspectos Legales Laborales
  - Supuesto: En cuanto que la gestión de los sistemas utilizados por los usuarios se realiza por un tercero el cumplimiento del deber de vigilancia de la actividad de los empleados por parte del usuario se ve limitada.

    Por otro lado, el Proveedor debe comprobar el adecuado uso de los servicios por parte de los empleados del Usuario.

    Riesgo de intromisión en los derechos a la intimidad a trabajador.

    La posibilidad de acceder desde cualquier punto de conexión puede dar lugar:

    Uso fraudulento de la identidad de los usuarios finales.

Extracción de la información y violación de las obligaciones de confidencialidad.

- Soluciones jurídicas:
  - Implantación de un protocolo de uso de herramientas informáticas dirigido a los trabajadores en los que se informe:
    - Del uso que deben hacer de las aplicaciones ubicadas en la nube, tanto profesional como privado que dependerá de las características de la aplicación.
    - De la gestión de los nombres de usuario y contraseña.
    - De las consecuencias, sanciones, por un uso inadecuado.
    - De quien va a hacer el seguimiento y control de la actividad en la nube.
    - De la obligación de secreto por parte de los usuarios.
  - Redacción por vía contractual de las condiciones en las que se va a llevar a cabo el control por parte del

Proveedor (la actividad laboral, como del adecuado uso de las aplicaciones):

- Ámbito
- Proporcionalidad
- Medios no intrusivos
- Justificados
- Modo de creación de las evidencias electrónicas, conservación y procedimiento de aportación.

- Aspectos legales Procesales o Judiciales
  - Supuesto: La utilización de la nube puede producir una deslocalización de la información y de la custodia de los datos o de la información, pudiendo ser custodiado por diferentes entidades.
  - Soluciones jurídicas:
    - Necesario preparas un procedimiento para gestionar la creación de evidencia electrónicas validas en juicio y un protocolo de actuación que regule la solicitud de las mismas bien por parte de la administración o bien por parte del cliente.
    - Creación de una base de datos central de conocimiento en el uso de la nube identificando quien custodia los

datos, que tipo de datos son, y el uso que se realiza de los mismos. El objetivo es poder tener una idea de la ubicación de los datos para cubrir las necesidades de acceso a los mismos en supuestos de litigios o aportación de los mismos a juicio.

- Los contratos de la nube que supongan una creación, uso o almacenamiento de datos en un tercero deberán incluir las siguientes previsiones:

    - Aclara la propiedad de los datos.
    - Acceso a los datos: quien, cuando, donde y como.
    - Coste para la identificación o búsqueda de la información.
    - Retención de datos: mínimo y máximo de retención, formato.
    - Destrucción y/o procedimiento de devolución de datos y verificación.
    - Almacenamiento de datos, segregación y requisitos de seguridad.
    - Descubrimiento y/o reunión y concesión de participación.

- Capacidad de conservación: identificación, ubicación, recuperación, grabación.
- Auditoria de cumplimiento de los extremos anteriores.
- Penas por incumplimiento.

- Aspectos Legales Propiedad intelectual (I)
  - Supuesto: Los usuarios querrán acceder y usar la nube en sus propios términos. Beneficiándose del acceso y uso a los servicios, contenidos, software que proporciona el proveedor en la nube y de su deslocalización, pero también querrán que su propia propiedad intelectual sobre sus contenidos y software creados en la nube y/o almacenados en ella sea protegida.
  - Soluciones jurídicas:
    - Incluir en el contrato y en la política de uso de o acceso a la nube las condiciones para establecer ese equilibrio entre la responsabilidad debida por los usuarios al ejecutar y usar los contenidos, servicios y software ajenos desde la nube, y las medidas de seguridad y protectoras de la PI de los usuarios a garantizar por proveedor.

- Aspectos Legales Propiedad intelectual (II)
    - Supuesto: La utilización de las aplicaciones alojadas en la nube puede dar lugar a la generación de creaciones intelectuales merecedoras de protección en materia de propiedad intelectual. Indefinición respecto a la titularidad de dichas creaciones intelectuales.
    - Soluciones jurídicas:
        - Incluir en el contrato el régimen de titularidad de derecho sobre las creaciones intelectuales que se incluyen en la nube.
- Aspectos Legales Propiedad intelectual (III)
    - Supuesto: La deslocalización, propia de la nube, puede dar lugar a la utilización del contenido ajeno, software ajeno o de los servicios que prestan a través de esta desde jurisdicciones donde está prohibido su uso o no se encuentra autorizado.
    - Soluciones jurídicas:
        - Necesario incluir en el contrato las restricciones de uso de la nube respecto de aquellos territorios desde donde no resulta viable, y establecer el mecanismo de control electrónico para que ese contenido o software ajeno no se puede ejecutar en tales territorios.

        - O bien renegociar y ampliar las licencias existentes entre los terceros proveedores de software, contenidos o servicios y el proveedor de servicios en la nube, para sus usuarios puedan desde cualquier jurisdicción.

- Aspectos Legales Propiedad Intelectual (IV)
    - Supuesto: La posibilidad que el usuario utilice:
        - El servidor en la nube para poner contenidos y software ajenos a disposición de terceros.
        - El servicio de almacenamiento remoto para almacenar una copia de contenidos y software, desde la que hacer reproducciones.
        - Así, los usuarios ponen al proveedor de estos servicios en la nueve en riesgo de responsabilidad legal por las infracciones de propiedad intelectual que con ello comentan.
    - Soluciones jurídicas:
        - Necesario incluir en el contrato la asunción expresa e inequívoca por parte de los usuarios de toda responsabilidad por estos actos potencialmente ilícitos.
        - Establecer en el contrato y en la política de uso de servicios en la nube que su proveedor se reserva la

facultad de monitorizar y eliminar los contenidos y software ajenos que los usuarios suban a la nube, en atención a criterios que afecten a derechos de terceros, intereses públicos, etc.

2.2 Seguridad

Alianza de Seguridad para la Nube, siglas en inglés (CSA) está diseñada específicamente para proporcionar los principios fundamentales de seguridad para guiar a los proveedores de nubes y para ayudar a los clientes en la nube prospectivos para evaluar el riesgo general de seguridad de un proveedor de la nube.

Dicha organización proporciona un marco de referencia de controles de seguridad, dividida en 12 dominios que descansan en una matriz personalizada con otros estándares aceptados por la industria de seguridad, regulaciones y controles de marcos como la ISO 27001/27002 (estándar para la seguridad de la información), ISACA COBIT (Objetivos de control para información y tecnologías relacionadas), PCI (Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago), NIST (El Instituto Nacional de Normas y Tecnología), Foro y NERC CIP (Protección de Infraestructuras Criticas) y aumentarán o proporcionar la dirección de control interno para el control de la organización de servicio informes certificados proporcionados por proveedores de la nube.

Los doce dominios son los siguientes:

1. **Gobierno y gestión de riesgo empresarial**

Capacidad de una organización para regular y medir el riesgo de la empresa presentado por la computación en la nube (cloud computing).Artículos legales toman precedencia en dado caso se viole el complimiento de acuerdo, la capacidad de las organizaciones de usuarios para evaluar adecuadamente el riesgo de un proveedor en de la nube, la responsabilidad de proteger los datos sensibles cuando ambos usuarios y proveedores pueden tener la culpa, y cómo las fronteras internacionales pueden afectar a estas cuestiones

2. **Cuestiones legales: Contratos y descubrimiento electrónico**

Posibles problemas legales al utilizar la computación en nube. En esta sección se tocan temas que incluyen los requisitos de protección de los sistemas de información y computación, leyes de divulgación de violación de la seguridad, los requisitos regulatorios y de privacidad, leyes internacionales, etc.

3. **Cumplimiento y Auditoria**

Mantener y comprobar el cumplimiento cuando se utiliza la computación en nube. Asuntos relativos a la evaluación de cómo la computación en nube afecta el cumplimiento de las políticas de seguridad interna, así como los diversos requisitos de cumplimiento (normativos, legislativos y de otro tipo) se discuten aquí. Este dominio incluye una cierta dirección en demostrar el cumplimiento durante una auditoría.

4. Gestión de la información y seguridad de los datos

La gestión de los datos que se colocan en la nube. Elementos que rodean la identificación y control de los datos en la nube, así como los controles de compensación que pueden ser utilizados para hacer frente a la pérdida de control físico al mover datos a la nube, se discuten aquí.

Se mencionan otras partidas, como quién es responsable de la confidencialidad, integridad y disponibilidad.

5. Portabilidad e Interoperabilidad

La capacidad de mover datos /servicios de un proveedor a otro e introducir nuevamente la información por completo nuevamente a la empresa o al usuario. Junto a cuestiones relacionadas con la interoperabilidad entre los proveedores.

6. Seguridad Tradicional, Continuidad del Negocio y Recuperación de Desastres

Cómo computación en la nube (cloud computing) afecta a los procesos operativos y procedimientos actualmente utilizados para implementar la seguridad, continuidad del negocio y recuperación ante desastres. El objetivo en este dominio es discutir y examinar los posibles riesgos de la computación en la nube, con la esperanza de aumentar el diálogo y el debate sobre la abrumadora demanda de mejores modelos de gestión de riesgos empresariales.

Además, en esta sección ayuda a las personas a identificar donde la computación en la nube puede ayudar en la disminución de ciertos riesgos de seguridad, o implica aumentos en otras áreas.

7. Centro de Datos

En este dominio se evalúa la arquitectura y las operaciones de centro de datos de un proveedor. Esta se centra principalmente en ayudar a los administradores a identificar características comunes de centros de datos que podrían ser perjudiciales a los servicios en curso, así como características que son fundamentales para la estabilidad a largo plazo.

8. Respuesta a Incidentes, notificación y Remediación

Adecuada detección de incidentes, respuesta, notificación y la remediación. Esta trata de abordar los elementos que deben estar en su lugar, tanto a nivel de proveedores y de los usuarios para permitir la gestión de incidentes y análisis forense adecuado. Este dominio le ayuda a entender las complejidades de la nube. Trae a su actual programa de manejo de incidentes

9. Seguridad de aplicaciones

Asegurar la aplicación de software que se ejecuta en o se están desarrollando en la nube. Esto incluye artículos tales como si es adecuado para migrar o diseñar una aplicación que se ejecute en la nube, y si es así, qué tipo de plataforma en la nube es más apropiado.

10. Cifrado y administración de llaves

Identificar el uso de cifrado apropiado y gestión de claves escalable. En esta sección no es prescriptiva, sino es más informativa, en la cual se discuten las necesidades y se identifican los problemas que surgen en el uso, tanto para la protección del acceso a los recursos como para la protección de los datos.

11. Identidad y control de acceso

Gestión de identidades y el aprovechamiento de los servicios de directorio activo proporciona un control de acceso. La atención se centra en los problemas encontrados al extender la identidad de una organización en la nube. En esta sección se ofrece información sobre el grado de preparación de la organización para llevar a cabo la identidad basada en la nube, Derecho y Administración de Acceso, sus siglas en inglés (IDEA).

12. Virtualización

El uso de la tecnología de virtualización de la computación en nube. El dominio se ocupa de temas como: los riesgos asociados a múltiples clientes, aislamiento equipos virtuales (Virtual Machine), co-residencia, las vulnerabilidades de hipervisor, etc. Este dominio se centra en los problemas de seguridad que rodean la virtualización del sistema / hardware, en lugar de un estudio más general de todas las formas de virtualización. Como marco, la Alianza de Seguridad para la Nube (Cloud Security Alliance) ofrece a las organizaciones la estructura necesaria, el detalle y la claridad en relación con la seguridad de

información adaptada a la industria de la nube. Consolida entornos de control de seguridad de la información existente, haciendo hincapié en los requisitos de control de seguridad de información de negocio, reduce e identifica las amenazas de seguridad consistentes y vulnerabilidades en la nube, ofrece la seguridad estandarizada y la gestión del riesgo operacional, trata de normalizar las expectativas de seguridad, la taxonomía de nubes, la terminología y medidas de seguridad implementadas en la nube.

Con la aparición de la computación en la nube como tecnología preferida para las operaciones de Tecnología de la Información (TI) de los contratistas, los problemas de seguridad en este el modelo de hospedaje han cobrado mayor importancia y criticidad.

Modelo de Seguridad para la Nube

El modelo de referencia de seguridad en la nube se ocupa de las relaciones de estas clases y los coloca en el contexto de sus correspondientes controles y las preocupaciones de seguridad.

Para las organizaciones y los individuos que se enfrentan a la computación en la nube, por primera vez, es importante tener en cuenta lo siguiente para evitar errores y confusiones posibles:

- La noción de cómo se implementan los servicios de nube, se utiliza a menudo de manera intercambiable con el lugar donde se prestan, lo que

puede llevar a confusión. Las nubes públicas o privadas pueden ser descritos como externa o interna, que puede no ser precisa en cualquier situación.

- La forma en que se consumen los servicios en la nube se describe a menudo en relación con la localización de la dirección de una organización o perímetro de seguridad. Aunque todavía es importante saber dónde se encuentran los límites de seguridad en cuanto a la computación en nube, la noción de un perímetro bien delimitado es un concepto anacrónico para la mayoría de las organizaciones.
- La re-perimetrización y la erosión de los límites de confianza ya están teniendo lugar en la empresa se amplifican y aceleran por la computación en la nube (cloud computing). Conectividad ubicua, la naturaleza amorfa de intercambio de información, y la ineficacia de los controles de seguridad estáticas tradicionales que no pueden hacer frente a la naturaleza dinámica de los servicios en la nube, todos requieren nuevas formas de pensar con respecto a la computación en la nube.

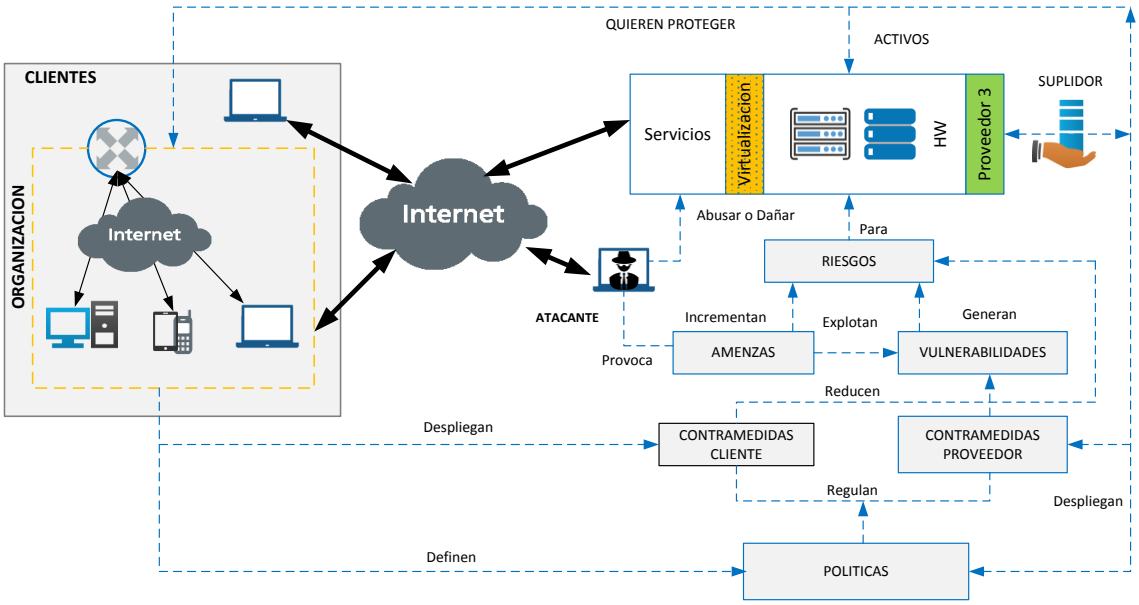


Grafico 6. Esquema básico de seguridad en un entorno de nube pública. Fuente propia basada en el libro Cloud Computing, Tecnología y Negocio.

Las modalidades de implementación y de consumo de la nube se debe pensar no sólo en el contexto de la "interna" versus "externo" en su relación con la ubicación física de los activos, los recursos y la información, sino también por los que se consumen, y que es responsable de su gestión, la seguridad y el cumplimiento de políticas y normas.

Esto no es para sugerir que el sobre o fuera de la premisa de la ubicación de un bien, un recurso o información no afecta a la seguridad y el riesgo de la postura de la organización porque lo hacen pero es importante tomar en cuenta que estos riegos dependen de:

- Los tipos de activos, los recursos y la información que se gestiona.
- Quién los administra y cómo los administra.

- Que se seleccionan como los controles y cómo se integran.

Según La norma de seguridad ISO / IEC 27002, apartado 6.2, por "Partes externas" controlar estados objetivos: "... la seguridad de la información de la organización y las instalaciones de procesamiento de información no debe ser reducido por la introducción de productos o servicios de externos..."

Por lo tanto, las diferencias en los métodos y responsabilidades para asegurar los tres modelos de servicio en la nube significan que los consumidores de servicios en la nube se enfrentan a una tarea difícil.

A menos que, los proveedores de nube pueden revelar fácilmente sus controles de seguridad y la medida en que se implementan para el consumidor y el consumidor sabe que se necesitan controles para mantener la seguridad de su información, hay un enorme potencial para las decisiones de gestión de riesgos equivocados y resultados perjudiciales.

En primer lugar, uno clasifica un servicio en la nube contra el modelo de arquitectura de nube. Entonces es posible mapear su arquitectura de seguridad, así como negocio, regulatorios, y otros requisitos de cumplimiento en contra de ella como un ejercicio de pre-evaluación (Gap Análisis). El resultado determina la "seguridad" la postura general de un servicio y cómo se relaciona con los requisitos de garantía y protección de un activo.

El grafico 7 muestra un ejemplo de cómo un mapeo servicio en la nube puede ser comparada con un catálogo de controles de compensación para determinar qué controles existen y cuáles no - conforme a lo dispuesto por el consumidor, el proveedor de servicio en la nube, o de un tercero. Esto a su vez puede ser comparado con un marco de cumplimiento o conjunto de requisitos, tales como PCI DSS, como se muestra.

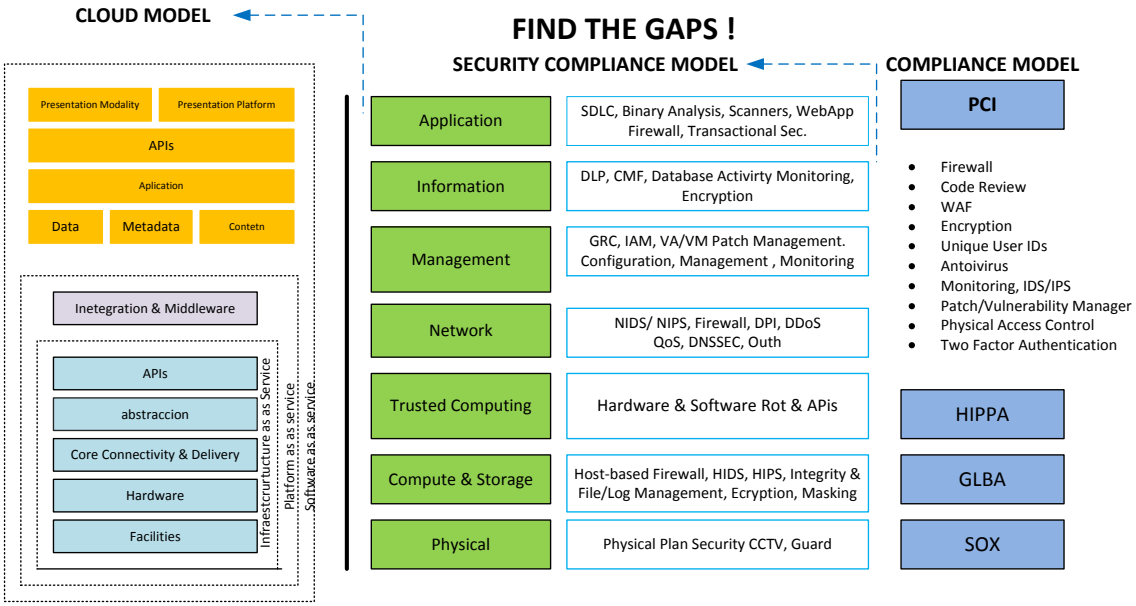


Grafico 7. Lineamiento de Seguridad para Áreas Criticas Focalizado en la Computación en la Nube. Fuente; Propia basada en la Alianza para la Seguridad en la Nube, siglas en inglés (CSA).

Una vez que este análisis de la brecha se ha completado, según las necesidades de cualquier mandato de cumplimiento normativo o de otro tipo, se hace mucho más fácil determinar lo que hay que hacer con el fin de retroalimentar a un marco de evaluación de riesgos. Esto, a su vez, ayuda a determinar cómo deben abordarse las carencias y en última instancia, los

riesgos: aceptadas, transferirse ni mitigados. Es importante tener en cuenta que el uso de la computación en nube como un modelo operativo no proporciona lograr el cumplimiento. La capacidad de cumplir con cualquier requisito es un resultado directo del modelo de servicios y el despliegue utilizado y el diseño, la implementación y la gestión de los recursos en la nube.

¿Qué es la Seguridad para el Cloud Computing?

Los controles de seguridad en la computación en nube no son diferentes de los controles de seguridad en cualquier entorno de Tecnología de la Información (TI). Sin embargo, debido a los modelos de servicio de nube empleadas, los modelos operativos y las tecnologías que se utilizan para habilitar los servicios en la nube, puede presentar diversos riesgos a una organización de soluciones de Tecnología de la Información (TI) tradicionales.

La postura de seguridad de una organización se caracteriza por la madurez, la eficacia y la exhaustividad de los controles de seguridad ajustadas al riesgo implementadas. Estos controles se implementan en una o más capas que van desde las instalaciones (seguridad física), a la infraestructura de red (seguridad de la red), a los sistemas de información (sistema de seguridad), hasta llegar a la información y las aplicaciones de seguridad (aplicaciones). Además, los controles se aplican a la gente y los niveles del proceso, tales como la separación de funciones y la gestión del cambio, respectivamente.

Cumplimiento y Normativa

Movidos por la necesidad de proteger los datos privados (información personal, datos financieros y los informes médicos) de las organizaciones frente a ciberdelicuentes y ladrones de identidades, gobiernos de todo el mundo han hallado agujeros normativos en todos los niveles. Las prácticas recomendables de la seguridad de la información están siendo codificadas con rapidez mediante mandatos legales que buscan garantizar que la política corporativa, los controles internos, los procesos comerciales y las operaciones empresariales de los distintos sectores se encuentren a salvo.

Existen más de 400 normas y más de 10,000 controles con presencia en más de 50 países de todo el mundo, el cumplimiento normativo se ha convertido en un gran reto y un mandato complejo para la organización. Estas normas a menudo requieren de controles específicos, programas corporativos de cumplimiento normativo, auditorías y procesos de divulgación pública, e imponen severas sanciones por incumplimiento. Éstas son algunas de las normas más relevantes sobre la seguridad de la información y los datos:

- **Ley Federal Sobre Gestión de la Seguridad de la Información (FISMA):** aplicable a las agencias y contratistas del gobierno de los EE. UU. Exige la aplicación de los procesos de seguridad de la información de acuerdo con las normas federales de procesamiento de la información, siglas en inglés (FIPS) y el instituto nacional de normas y tecnología siglas en inglés (NIST).

Las FISMA precisa de evaluaciones periódicas de riesgo, incluida la magnitud del daño que podría resultar en caso de acceso, uso, revelación, interrupción, modificación o destrucción no autorizada de la información y sistemas de información.

Contempla políticas, procedimientos, pruebas, planes de acciones correctivas e información, basándose en valoraciones de riesgos, para garantizar que la seguridad de la información abarca todo el ciclo de vida de cada uno de los sistemas de información de la organización.

- **Ley de Transferibilidad y Responsabilidad de los Seguros Médicos (HIPAA):** estas reglas de seguridad y privacidad son aplicables a las "entidades afectadas y sus socios comerciales de la industria sanitaria."

Las Normas para la privacidad de los datos individualmente identificables de la Salud ("Regla de Privacidad"), establece, por primera vez, un conjunto de normas nacionales para la protección de cierta información de salud.

El Departamento de Salud y Servicios Humanos de los EE.UU. ("HHS") emitió la Norma de Privacidad para cumplir el requisito de la Ley de Responsabilidad de 1996 ("HIPAA") y Portabilidad de Seguros de Salud. Atender las normas Regla de Privacidad al uso y divulgación de la información de salud de las personas llamada "información médica protegida (PHI)" por las organizaciones sujetas a la

Regla de Privacidad - llamadas "entidades cubiertas", así como normas para los derechos de privacidad de los individuos para comprender y controlar cómo se utiliza su información de salud. Dentro de HHS, la Oficina de Derechos Civiles ("OCR") tiene la responsabilidad de aplicar y hacer cumplir la Regla de Privacidad con respecto a las actividades de cumplimiento voluntario y multas civiles.

- **Ley de Tecnología de la Información Sanitaria para la Salud Económica y Clínica (HITECH):** proporciona, entre otras cosas, fondos para la financiación de historias clínicas digitales (HCE) y exclusión de responsabilidad ante peticiones de divulgación relacionadas con la violación de información cifrada.

Con esta ley, los socios de negocios son ahora responsables de la privacidad y los requisitos de seguridad que anteriormente sólo estaban obligados por las entidades cubiertas. Además, un socio de negocios está sujeto a sanciones civiles y penales. Esto también incluye una disposición que permite a los pacientes recibir una compensación económica por la violación de su privacidad.

La ley exige que las sanciones monetarias civiles o acuerdos monetarios como resultado de una violación de las reglas se envíen a la Oficina de Derechos Civiles (OCR) para la ejecución de la privacidad y normas de seguridad. Sanciones monetarias civiles tienen ahora un sistema de niveles que van desde

$ 100 a $ 50.000 U.S. dependiendo de la ofensa. El Secretario de HHS se requiere para llevar a cabo auditorías periódicas para asegurarse de que las entidades cubiertas y socios de negocios cumplen con las nuevas normas. La Ley HITECH ha hecho que el uso de la encriptación lo único que proporciona un "puerto seguro" para no tener una brecha. Los datos que no estén cifrados se consideran garantizados de acuerdo con la ley.

Debe haber políticas y procedimientos escritos, un análisis de riesgos, también tener un plan de contingencia para cualquier tipo de interrupción del negocio. El sistema también tiene que proporcionar pistas de auditoría para que tenga acceso a la información de salud protegida. Las reglas requieren capacitación de la fuerza laboral, lo que debe hacerse y documentarse.

Norma de Seguridad de Datos de la Industria de las Tarjetas de Pago (PCI DSS): mandato industrial que establece los requisitos de seguridad de la información para organizaciones que procesan transacciones con tarjeta (tales como las tarjetas de crédito y débito).

Las Normas de Seguridad de Datos (DSS) de la Industria de Tarjetas de Pago (PCI) se desarrollaron para fomentar y mejorar la seguridad de los datos del titular de la tarjeta y para facilitar la adopción de medidas de seguridad consistentes a nivel mundial.

Los requisitos de seguridad de las DSS de la PCI rigen para todos los componentes del sistema. Los “componentes del sistema” se definen como todo componente de la red, del servidor o de la aplicación que se incluye en el entorno de los datos del titular de la tarjeta o que está conectado a éste.

El entorno de los datos del titular de la tarjeta es la parte de la red que posee los datos del titular de la tarjeta o los datos confidenciales de autenticación. Los componentes de la red incluyen, a modo de ejemplo, firewalls, interruptores, routers, puntos de acceso inalámbricos, aplicaciones de la red y otras aplicaciones de seguridad.

Los tipos de servidores incluyen, a modo de ejemplo: web, aplicación, base de datos, autenticación, correo electrónico, proxy, protocolo de tiempo de red (NTP) y servidor de nombre de dominio (DNS).

Las aplicaciones incluyen todas las aplicaciones compradas y ordinarias, incluidas las aplicaciones internas y externas (Internet).

- **Sarbanes-Oxley (SOX):** las empresas de capital abierto deben poner en práctica un sistema de control informático. Algunos mandatos no pueden ser llevados a cabo sin el uso prudente de la seguridad para la tecnología y la información.

La Ley Sarbanes-Oxley, conocida también como SarOx ó SOA (por sus siglas en inglés Sarbanes Oxley Act), es la ley que regula las funciones financieras contables y de auditoría y penaliza en una forma severa, el crimen corporativo y de cuello blanco. Debido a los múltiples fraudes, la corrupción administrativa, los conflictos de interés, la negligencia y la mala práctica de algunos profesionales y ejecutivos que conociendo los códigos de ética, sucumbieron ante el atractivo de ganar dinero fácil y a través de empresas y corporaciones engañando a socios, empleados y grupos de interés, entre ellos sus clientes y proveedores.

2.3 Interoperabilidad Datos y Aplicaciones

Según el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) define interoperabilidad como la habilidad de dos o más sistemas o componentes para intercambiar información y utilizar la información intercambiada. En una definición más entendible la interoperabilidad permite que recursos de distintos formatos, plataformas de hardware y software puedan ser compartidos entre sí. Entre los beneficios de interoperabilidad se destacan:

- La interoperabilidad obliga a estructurar y normalizar la información lo que mejora la rapidez y la fiabilidad.
- Se minimizan los datos registrados manualmente, en papel o el intercambio verbal, aumenta su seguridad.
- Se reducen duplicidades y se mejora el tiempo resolución en un proceso clínico.

2.4 Portabilidad

Hoy día las aplicaciones en la nube no están diseñadas solamente para accederla desde el computador, sino también desde dispositivo móviles, empresas internacionales como Google, Dropbox, McAfee se han preocupado por llevar estas aplicaciones a los dispositivos móviles, en nuestro país empresas como Tpago, Banco Popular, Banco Leon, Carribean, páginas amarillas han incursionado en proveer aplicaciones de consulta y transaccionales a la plataforma móvil. Apple Computer fue una de las empresas pioneras en motivar a que las empresas e individuos desarrollaran aplicaciones para dispositivos móviles tales como: tabletas electrónicas y teléfonos celulares según el estudio realizado por Apple en su tienda en línea existen más de 850,000.00 aplicaciones y han sido descargadas 10 billones de aplicaciones.

Fuente:http://www.apple.com/pr/library/2013/05/16Apples-App-Store-Marks-Historic-50-Billionth-Download.html.

Ante estas estas facilidades de conexión surgió la necesidad de proteger la información del negocio en el teléfono personal del individuo, lo que motivo a las empresas como Airwacth, Mobiliron, Citrix a desarrollar aplicaciones para asegurar la información del negocio y al mismo tiempo proveer a los usuarios internos como externo de la empresa al uso de aplicaciones públicas o privadas, administración del dispositivo y el contenido que pueda tener el mismo.

Según la firma analista Forrester evaluó en su reporte a 16 de los proveedores más importantes, basado en actual oferta, estrategia y presencia en el mercado. El reporte se enfoca en proveedores cuyos productos están en su mejor momento, que están estratégicamente comprometidos con el mercado y que tienen permanente presencia en las listas de preseleccionados de los departamentos de Tecnología de la Información corporativos cuando estos van a realizar la adquisición de un producto para sus empresas.

Tan sólo para ser considerados en el reporte, los proveedores debían ser capaces de manejar dos actividades fundamentales: gestionar la sincronización de archivos en múltiples tipos de dispositivos y permitir el intercambio de contenido entre colegas y usuarios dentro y fuera de una organización.

Forrester incluyó a AirWatch dentro de su lista y lo destacó por su sólido desempeño otorgándole la máxima calificación posible por su modelo de seguridad, “Organizaciones a lo largo del mercado están tratando de identificar el proveedor más adecuado para la implementación de sus estrategias de contenido móvil, y este reporte -proveniente de una de las firmas de analistas más importantes- valida el sólido desempeño que tenemos en la industria”, dijo John Marshall, presidente y CEO de AirWatch. “Nuestra estrategia siempre ha sido ofrecer a los clientes la mayor flexibilidad durante la ejecución de sus iniciativas móviles.

Continuamos diferenciándonos de los proveedores tradicionales y añadiremos aún más funcionalidades adicionales para acelerar el desempeño de nuestra plataforma en el próximo trimestre

".Fuente: http://www.air-watch.com/resources/analyst-reports/the-forrester-wave-file-sync-and-share-platforms-q3-2013/form Forrester The Forrester Wave™: File Sync And Share Platforms 2013

En el caso de la continuidad de negocio basado en la nube existen un sin número de empresas los cual proveen la administración y monitoreo de soluciones para el monitoreo de servicios en la nube la cual le da la facilidad a los administradores de Tecnología de la Información (TI) verificar si los sistemas están en línea, si existe alguna falla o si ha ocurrido algún evento relevante, y todo administrado desde un dispositivo móvil.

Empresas como CISCO indican que durante el pasado año, la insistencia de los usuarios finales para aprovechar sus tablets y smartphones a fin de aumentar la productividad, incluso aunque ello suponga que ellos mismos deban adquirir los nuevos dispositivos, ha hecho que muchos departamentos de Tecnología de la Información (TI) adopten políticas menos restrictivas para permitir a los empleados funciones básicas de conectividad o, cada vez más, el acceso total a la red de TI y a las aplicaciones corporativas. Esta tendencia es probablemente irreversible y las organizaciones de TI deberán adaptarse rápidamente al fenómeno de los dispositivos de consumo.

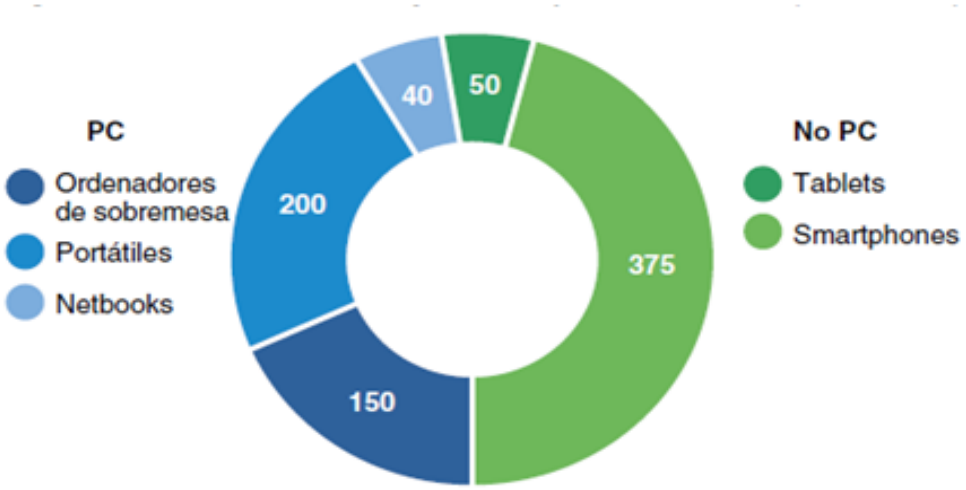


Grafico 8. Ventas de PC y otros dispositivos en 2011(en millones) Fuente Deloitte 2011

Otro estudio refleja cuanto mayor sea el número de empleados que puedan acceder fácilmente a sus aplicaciones de trabajo mediante redes móviles y Wi-Fi, más se extenderán estas redes y, por tanto, mayor será la posibilidad de acceso.

El resultado final es la conectividad permanente en cualquier lugar y en todo momento, y ello supone que las redes corporativas tendrán más dispositivos conectados con mayor frecuencia y será necesario por tanto que las aplicaciones estén disponibles de forma ininterrumpida.

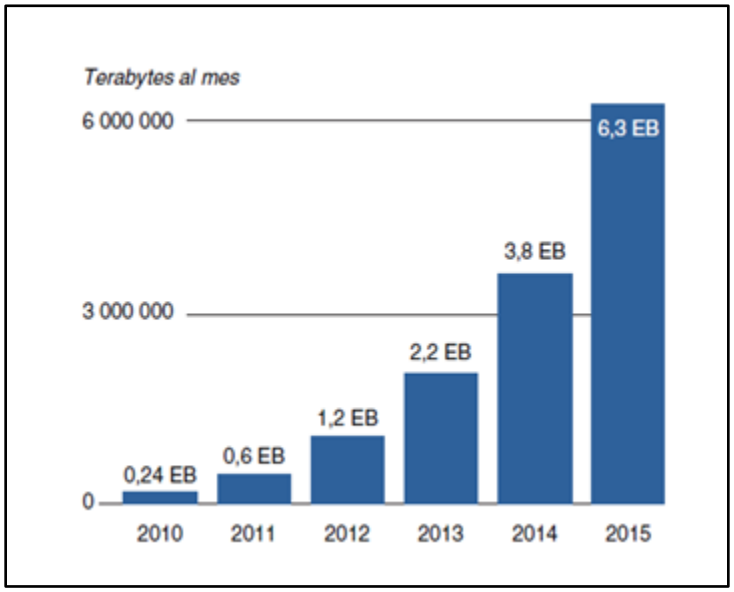


Grafico 9. Reporte mundial de consumo de datos de dispositivos móviles.
Fuente: CISCO Visual NetworkingIndex 2011

Es importante tener en cuenta que existen diferentes segmentos de usuarios en cualquier implementación de uso de dispositivos personales o trae tu propio dispositivo, siglas en inglés (BYOD). Se recomienda realiza un análisis de los segmentos de usuarios dentro de la empresa para poder entender las necesidades y el nivel de soporte necesarios tal y como se muestra en el grafico 10.

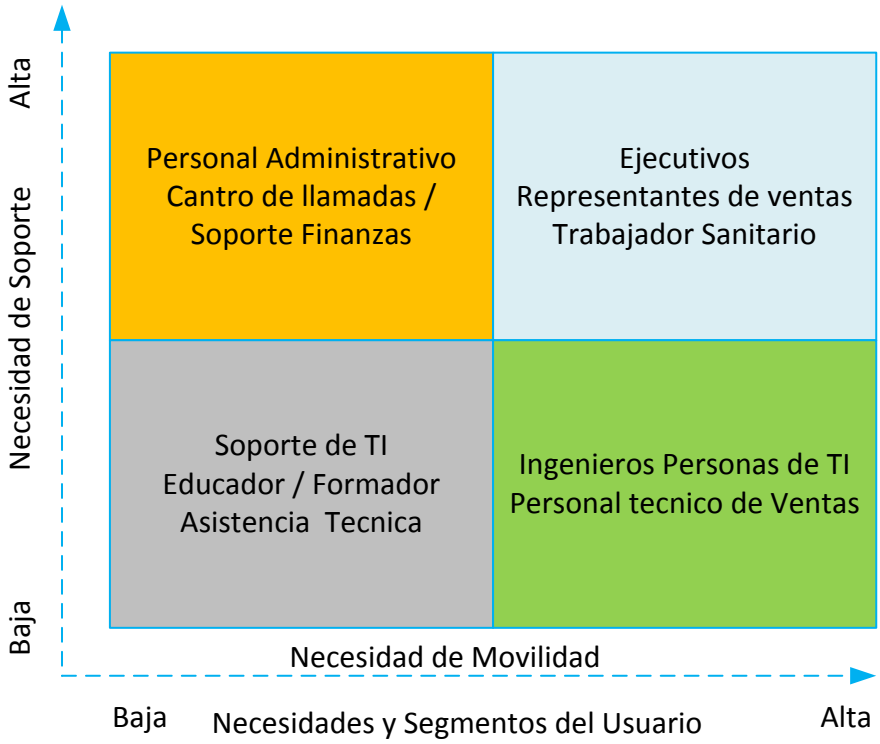


Grafico 10.Necesidades y Segmentos del Usuario. Fuente Propia Basada en Cisco.

Cada empresa es diferente. El grafico 10 analiza las funciones de los empleados teniendo en cuenta las necesidades de movilidad y aplicaciones móviles, y el probable nivel de soporte que necesitarán. Las implementaciones de trae tu propio dispositivo, siglas en inglés (BYOD), son sencillas en el caso de usuarios que solo requieren niveles bajos de asistencia de Tecnología de la Información (TI) y que probablemente utilizan comunidades de auto asistencia en las que se comparten las mejores prácticas. Las implementaciones serán más complejas con usuarios con mayor necesidad de movilidad y que necesitarán un mayor nivel de asistencia, como en el caso de ejecutivos.

Realizar este tipo de análisis ayudará a comprender las políticas de derechos y los modelos de asistencia, y puede evitar frustraciones y gastos excesivos del presupuesto de Tecnología de la Información (TI).

El uso de las nuevas tecnologías puede ser regulado por la empresa dentro de su rango de acción, y es que la utilización de los móviles particulares durante la jornada laboral pueden resultar un problema para la productividad e incluso para la seguridad de los trabajadores, en según qué puestos.

Esta regulación interna puede incluirse en los nuevos contratos de trabajo mediante una cláusula específica, además de poder ser expuesta a los trabajadores ya contratados para que firmen el conocimiento de estas normas internas. Eso sí, se debe aplicar de forma no discriminatoria.

Fuente:http://www.bbvacontuempresa.es/recursos-humanos/clausula-contractual-sobre-el-uso-del-movil-la-empresa.

2.5 Gobernabilidad y Gestión

La gobernabilidad de la nube implica aplicar políticas para utilizar los servicios de nube. Puede ser útil pensar en la gobernabilidad de la nube analizando su opuesto, el caos gratuito para todos, en el cual una organización utiliza los servicios de nube sin tener la supervisión adecuada. Para evitar esto, se deben aplicar políticas para el uso de los servicios de nube para controlar la fuga de información privada a la nube y el uso excesivo de los servicios de nube.

- **Gobernabilidad de SOA (Arquitectura Orientada a Servicios)**

Gobernabilidad es una palabra que cobró vida con la adopción de la arquitectura SOA. En el mundo de SOA, la gobernabilidad está dividida en tiempo de diseño (definición de políticas para los servicios web) y tiempo de ejecución (en realidad, la aplicación de esas políticas al tráfico en tiempo real).

En la mayoría de los casos se accede a las plataformas de nubes, como a los servicios de una arquitectura SOA, utilizando las API de servicios web, y, por lo tanto, deberían estar dentro del mismo encabezado que la gobernabilidad de SOA. Como mínimo, podemos utilizar los principios en los que se basa la gobernabilidad de SOA.

A menudo, la gobernabilidad de SOA depende de la presencia de un registro. Es un lugar central al que puede dirigirse el usuario para ver los servicios de la plataforma SOA y las políticas aplicables a esos servicios. La política de servicios web estándar, así como la especificación Servicio Web Adjunto (WS-Attachment) complementaria, permite asignar una política a un servicio en una arquitectura SOA. En realidad, el servicio contiene un “indicador” para su política. El registro administra la relación entre los servicios y las políticas.

Otra función importante de los productos de gobernabilidad de SOA es la gestión del ciclo de vida de los servicios. Que no es más que la capacidad para controlar y realizar un seguimiento de los cambios al servicio, y colocar los controles

sobre los que pueden realizar estos cambios. Una vez instaurada esta facilidad, una organización puede determinar quién creó el servicio, quién lo modificó y cuándo se produjeron los cambios.

Los servicios enviados hacia y desde los servicios de nube generalmente no son Protocolo simple de acceso a objetos siglas en inglés (SOAP) y los servicios con frecuencia no están definidos por la descripción de lenguaje de servicio web por su siglas en inglés (WSDL), que son dos de los estándares utilizados en la gobernabilidad de SOA en la mayoría de los casos. Esto significa que importar los servicios a un registro de gobernabilidad de SOA no es una tarea directa. Los servicios web utilizados por la computación en nube omiten a SOAP y WSDL y utilizan, en cambio, servicios livianos del estilo REST que son más populares entre los desarrolladores debido a su relativa simplicidad.

- **Gobernabilidad del Lado del Cliente**

Un proveedor de servicios de nube generalmente no tiene que comunicar con anticipación a los clientes el tiempo que el servicio estará inactivo. Además, cuando se produce la interrupción del servicio por causas imprevistas, el proveedor del servicio de la nube no tiene la obligación de comunicar este hecho a los usuarios del servicio de nube. Para monitorear el tiempo de respuesta y la disponibilidad de los servicios de nube, se requiere un componente del lado del cliente. Este componente (por ejemplo, una puerta de enlace XML) monitorea la conexión con la plataforma de la nube. Si la conexión es lenta, entonces la

puerta de enlace XML emite un alerta o toma una medida correctiva como el uso de respuesta de su caché. Si se utiliza el caché de esta manera, es posible mitigar los efectos de la interrupción del servicio de nube.

La puerta de enlace XML en el cliente también puede escanear los datos destinados a la nube en busca de fugas de información privada o sensible para la empresa. Además, habría que encriptar, o encriptar selectivamente, los datos antes de enviárselos al proveedor de nube.

Por ejemplo, una puerta de enlace XML podría garantizar que los datos que ingresan al proveedor de computación en nube están desidentificados para que sea imposible asociar la información privada con los datos.

Las puertas de enlace XML, como la Edición XML Gateway Cloud de Vordel, filtran el tráfico que se envía a las plataformas de nube y aplican las políticas para acceder a los servicios de nube. Al hacerlo, las puertas de enlace XML brindan una vía de acceso al lado del cliente para los servicios de nube.

2.6 Medición y Monitoreo

Para garantizar rendimiento consistente de los sistemas virtuales se puede obtener información sobre las tendencias y cargas máximas vía la monitorización de la red.

Antes de moverse a una nube privada, un departamento de Tecnología de la Información (TI) debe considerar las demandas de rendimiento de las aplicaciones y las fluctuaciones cíclicas. El análisis de largo plazo, tendencias y cargas máximas se pueden obtener vía evaluaciones de la monitorización de la red y así planificar la disponibilidad de recursos de acuerdo a la demanda. Esto es necesario para garantizar un rendimiento consistente en los sistemas virtualizados.

Sin embargo, una nube privada solo funcionará sin problemas si una red altamente confiable conecta los servidores físicos. Por esta razón toda la infraestructura de la red debe ser analizada en detalle antes de crear una nube privada. Esta red debe satisfacer los requerimientos de velocidad de transmisión y estabilidad, en caso contrario deberán mejorarse el hardware o las conexiones de la red. Por último, perdidas menores en la velocidad de transmisión pueden llevar a disminuciones del rendimiento.

El administrador de Tecnología de la Información (TI) puede usar una solución de monitorización en la planificación de una nube privada. Si una aplicación (que usualmente equivale a varios servidores virtualizados) va a operar sobre varios servidores host (“cluster”) en la nube privada, necesitará usar una red de almacenamiento, siglas en inglés (SANs), la cual transporta los datos en la red como una solución central de almacenamiento. Esto hace aún más importante la monitorización del rendimiento de la red.

La falla de un solo equipo virtual que provee servicios a diferentes clientes puede interrumpir el acceso a 50 o 100 aplicaciones centrales. Los conceptos modernos de clustering se usan para tratar de evitar estas fallas, pero si un sistema falla a pesar de estos esfuerzos, se trata inmediatamente. Si un servidor host se cae arrastra consigo un gran número de máquinas virtuales o sus conexiones de red ponen lentas o se interrumpe, todos los servicios virtuales en ese host se ven afectados instantáneamente, lo que incluso con los mejores conceptos de clustering, muchas veces no se puede evitar.

Una solución de monitorización de red, ofrece notificaciones, instantáneas cuando se produce una interrupción dentro del ambiente Tecnología de la Información (TI), tanto en la compañía como en la nube.

Un operador o cliente debe proveer una solución de monitorización dentro de la nube privada y como resultado, el personal de Tecnología de la Información (TI) pueda monitorizar la nube privada de manera más precisa y directa que un servicio comprado en la red pública. Una nube privada permite acceso irrestricto cuando es necesario.

Esto permite a los administradores Tecnología de la Información (TI) hacer directamente un seguimiento de la condición de todos los sistemas relevantes con una solución privada de monitorización de red. Esto abarca la monitorización de cada máquina virtual, como también de los hosts y servidores

físicos, cortafuegos, conexiones de red, etc. Para mantener el servicio en la nube no solamente se deben enfocar si en los estados de los equipos están up o down, también existen otros factores que podemos monitorear y en base a esos resultados prevenir fallas o caídas del servicio.

Utilizar soluciones de monitoreo para que verifiquen los siguientes parámetros, por ejemplo, en cada servidor (virtual) que corre en la nube privada, como también los servidores host:

- Uso de CPU
- Uso de memoria (page files, swap file, page faults, etc.)
- Tráfico de la red
- Acceso al disco duro, espacio libre en disco y cantidad de lectura o escritura
- Parámetros de bajo nivel del sistema (ej.: largo de la cola del procesador, switches de contexto)
- Tiempo de respuesta http del servidor web

Procesos críticos como servidores SQL o servidores web, a menudo se monitorizan individualmente, en particular el uso de CPU y memoria. Adicionalmente, se puede monitorizar la condición del cortafuego (uso de ancho de banda, CPU). Si alguna de estas variables se encuentra fuera de un rango definido (ej.: Uso de CPU sobre 95% por más de 2 ó 5 minutos), la

monitorización enviará notificaciones al administrado. Una nube privada permite al administrador Tecnología de la Información (TI) monitorizar de cerca la condición de todos los sistemas relevantes con la solución de monitoreo la cual debe ser compatible con ambientes virtuales, a continuación en el grafico 11 se visualiza el diagrama de monitoreo en un ambiente virtual.

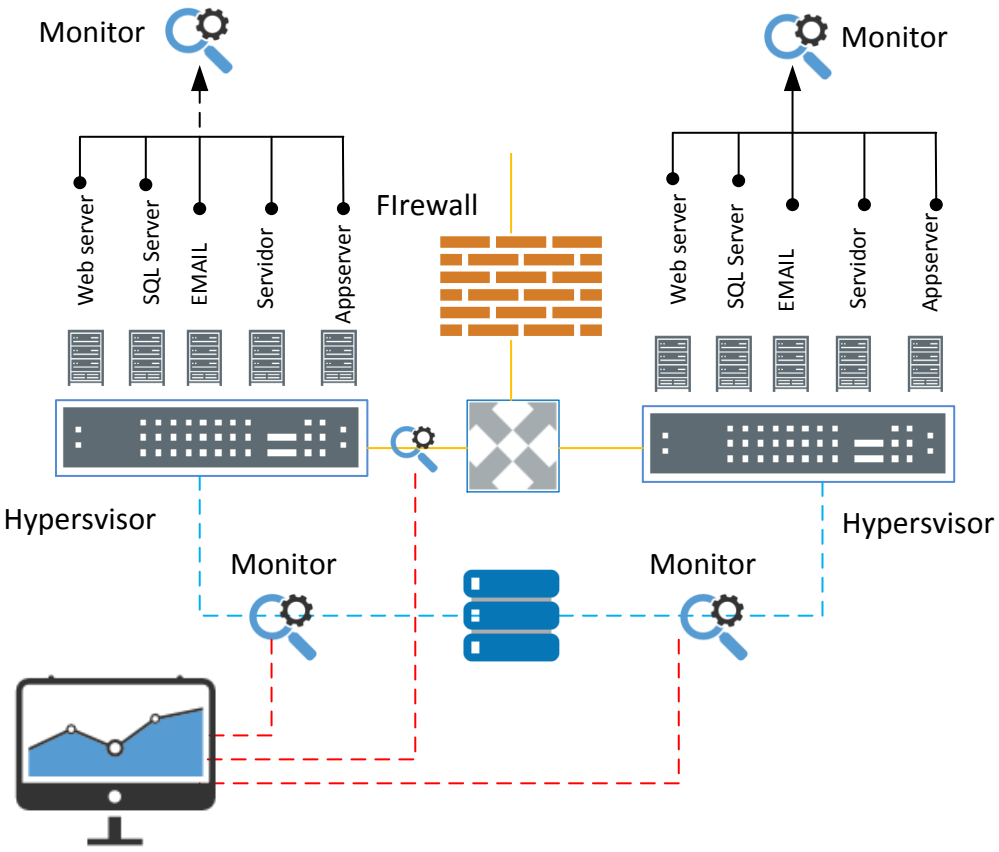


Grafico 11. Diagrama de monitoreo de estructura virtual: Fuente propia

Un operador de sitio web debe asegurar que todas las funciones están siempre disponibles a todos los visitantes, sin importar de cómo se haga técnicamente. Las siguientes preguntas son relevantes en este aspecto:

- ¿Está en línea el sitio web?
- El servidor web ¿entrega los contenidos correctos?
- ¿Qué tan rápido carga el sitio?
- ¿Es procesada correctamente la compra?

Estas preguntas solo se pueden responder si la monitorización de red se ubica fuera del servidor en cuestión. Idealmente, la monitorización debería operar fuera del centro de computación. Debería por lo tanto ser capaz de instalar una solución de monitorización de red en otro servidor de la nube u otro centro de computación. Es crucial que todos los lugares sean confiables y que un clúster de alta disponibilidad soporte la monitorización de manera que se garantice una monitorización sin interrupciones.

2.7 Acuerdo de Nivel de Servicio (Siglas en Ingles: SLA. Service Level Agreement)

- **Rendimiento, calidad y niveles de servicio**

Los principales agentes que intervienen en un entorno de la nube son los proveedores el cual suministran servicios, los intermediarios, que los gestionan y enriquecen y los clientes, que los disfrutan. Entre ellos debe establecerse una relación contractual en la que se especifiquen claramente y sin ambigüedades

las condiciones, mecanismos y términos que aseguren que la provisión, gestión y disfrute de los servicios en la nube se van a realizar de acuerdo a unas condiciones técnicas, legales y económicas acordadas entre las partes. A ese acuerdo se le denomina Acuerdo de Nivel de Servicios por sus siglas en ingles (SLA)y es una parte fundamental de todo contrato realizado entre agentes Cloud.

La SLA debe estar identificar y definir correctamente las necesidad del cliente en todos los ámbitos (tecnológicos, operativos, financieros y legales) proporcionar un marco para la comprensión mutua basado siempre que sea en criterios objetivos y métricas fácilmente cuantificables, sim planificar los aspectos de SLA.

Existen tres tipos de SLA predefinidas o Negociables, SLA predefinidas y parcialmente negociables y SLA particularizadas, las primeras son las que normalmente los proveedores de nubes públicas ofrecen un acuerdo para todos sus clientes, estos aceptan o no (sin poder mediar o cambiar ninguno de los conceptos o términos) en este caso la aceptación se realiza en muchas ocasiones a través de la misma Web en la que se contrata el servicio.

El tercer tipo de SLA completamente personalizada mediante una negociación entre ambas partes, son más parecidas a los acuerdos de externalización de servicios asociados a sistemas de información. En este caso, dado que en

estos momentos no existe un formato o plantilla estándar de SLA para entornos de nube. Dentro de los SLA se encuentran los acuerdos de descripción de servicios por sus siglas en inglés (SDA) debe incluir una pormenorizada relación de todos los servicios contratados por el cliente, su naturaleza y sus principales funcionabilidades, por tanto es necesario que en el acuerdo aparezca:

- Tipo de servicio contratado Infraestructura como servicio siglas en inglés (IaaS), plataforma como servicio siglas en inglés (PaaS), o programas como servicios siglas en inglés (SaaS).
- Identificar servicios que requieren una regulación sectorial especial o que por su naturaleza demanden determinadas particularmente en el ámbito de la seguridad, la accesibilidad, la monitorización o la audibilidad entre otros.
- Enumeración y cuantificación de los recursos de cómputos que el cliente tiene disponible para realizar sus transacciones.
- Se relaciones la interdependencia entre los servicios contratados y los procesos que permiten ofrecerlos. Por Ejemplo: No es posible obtener la disponibilidad pactada, si los procesos de gestión de capacidad de la demanda y aprovisionamiento no se diseñan y ejecutan correctamente.
- Se identifica los medios que tiene el cliente para disfrutar de soporte técnico en caso de que ocurra alguna incidencia. Así mismo, se debe determinar si existe soporte tiene un costo adicional o no.

- Se explican las políticas de mantenimiento, actualización y mejoras que desarrolla el proveedor, especificándose (si es posible) su alcance y prioridad.
- Se distinguen otro tipo de funcionabilidades que ayuden al cliente hacer un mejor uso de los servicios que el proveedor proporciona, como puede ser el acceso Interfaces de aplicaciones siglas en inglés (Api) específicas, la posibilidad para y restaurar los servicios de protección del cliente en particular.

Otras de las cosas que contempla el SLA es el objetivo de servicio siglas en inglés (SOA) se trata de establecer los objetivos de servicio que debe proporcionar el proveedor en la nube. Para ellos se suelen utilizar una serie de métricas o indicadores a las que se les vincula un valor específico o un rango de valores que determinan los objetivos.

Por lo tanto los SLA se deben definir basados en el SOA y en el SDA las cuales definen los siguientes:

- Los aspectos que permiten establecer los objetivos, las métricas que pueden utilizarse para cuantificar cada uno de los aspectos y los valores mínimos y máximos deseados para cada una de ellas , que son los que fijan los objetivos.
- Las metodologías de medición que van a utilizar el proveedor para corroborar si está cumpliendo con la SLA o no

- Los planes de contingencia que el proveedor pondrá en marcha si, por lo cualquier circunstancia, no pudiera cumplir con los objetivos fijados.
- La forma de integración de la gestión de la SLA por parte del proveedor con sus mecanismos de control de admisión, equilibrio de carga aprovisionamiento.
- Las normativas, metodológicas y/o prácticas que cumplen el proveedor en el ámbito de la seguridad (ISO 27001, SOC 1,2,y 3 por Ejemplo)
- El tiempo de respuestas que el proveedor prevé para corregir las nuevas vulnerabilidades que surjan asociadas a su infraestructura.
- La disposición del proveedor para que el cliente realice distintos tipos de auditorías de seguridad.

2.8 Virtualización de Aplicaciones

El propósito de esta tecnología es proveer al cliente un ambiente en la cual la aplicación no dependa del sistema operativo para ejecutarse, esta tecnología actualmente se está expandiendo a los dispositivos móviles también, existen dos empresas pioneras en ofrecer este tipo de tecnología VMWARE y CITRIX.

Según el reporte de IDC de abril 2012 indica que el primer enfoque de la virtualización fue usarlo para ambiente de prueba y desarrollo soportado en múltiples equipos virtuales, todo este proceso comenzó a cambiar en el 2005 y continúo acelerándose con la maduración de la tecnología de virtualización.

Durante el 2007 la segunda generación de virtualización (Virtualización 2.0) estaba alineada y enfocada en la consolidación de aplicaciones de producción. Hoy día las organizaciones están pasando por una transición a la era de la virtualización 3.0 en esta se está tomando el ambiente de la nube como atributo.

Las últimas plataformas de virtualización están combinadas con herramienta de administración, la fomentación de la creación de la nubes ofrecen plataformas agiles para aplicaciones.

La nube va más allá de la virtualización, ahora con aplicaciones en la nube, el personal de TI puede transformar las aplicaciones en un ambiente dinámico, de manera que los servicios de TI pueden reaccionar a los requerimientos del negocio. La virtualización de aplicaciones puede tener múltiples beneficios para Tecnología de la Información (TI) incluyendo:

- **Ahorro en costos:** Consolidación de hardware, energía eléctrica y sistemas de enfriamiento así como también en la fabricación del centro de datos.
- **Flexibilidad:** Desasociar la pila de software del hardware, lo que facilita las operaciones para las cosas tales como el mantenimiento planificado, lo que permite la infraestructura para ser reconfigurado, además de poder mover esto en la nube.

- **Empleados productivos:** Aumento de la eficiencia en la gestión, permitiendo que más servidores puedan ser administrados por el mismo administrador.

- **TI ágil:** la creación de un entorno de Tecnología de la Información (TI) adaptable, flexible y capaz de responder a las cambiantes necesidades de negocio al reducir el tiempo y esfuerzo necesarios para aprovisionar recursos o escalar una aplicación.

- **Simplificación de Operaciones:** Proporciona una plataforma para ofrecer servicios de infraestructura, tales como la optimización de recursos, alta disponibilidad, recuperación de desastres, o universalmente para las máquinas virtuales y las aplicaciones, lo que le permite simplificar las operaciones, reducir el número de habilidades que necesitan los de Tecnología de la Información (TI) e introducir una mayor coherencia a través de aplicaciones.

En resumen las incompatibilidades entre una aplicación y su sistema operativo se pueden abordar ya sea desde la virtualización del servidor o la de la presentación, pero cuando se trata de problemas de compatibilidad entre dos aplicaciones instaladas en el mismo elemento de un sistema operativo, necesitas recurrir a la virtualización de aplicaciones.

Un caso de éxito logrado por Microsoft en el centro médico North Shore situado en Massachusetts ejecutaba su sistema de tecnología clínica para médicos y enfermeras en un hardware y un software cada vez más viejo que conseguía frustrar a los profesionales de la medicina, hacer perder su precioso tiempo y recursos al departamento Tecnología de la Información (TI) para su mantenimiento y frenaba su capacidad para responder ante los nuevos requisitos del negocio.

Para sustituir este sistema, el centro adoptó una solución de cliente ligero para unidades móviles y de escritorio que utilizaba tecnologías Microsoft.

Los resultados fueron: iniciar la sesión llevaba segundos en lugar de minutos, se mejoró la fiabilidad.

Los costes de hardware y software se vieron recortados en un 30%; se espera que las peticiones de ayuda de escritorio se reduzcan en un 50%; y el coste total de propiedad ha caído en torno a un 30%.

Lo que es mejor aún, la solución proporciona a los doctores y a las enfermeras más tiempo para hablar entre ellos y con los pacientes, incrementado así la calidad de los cuidados.

2.9 Continuidad de Negocios Tecnología de la Información (Siglas en Ingles TI)

Dentro de la gestión de seguridad de la información en una organización es importante contar con un plan que garantice la continuidad de las operaciones de Tecnología de la Información (TI). Continuidad de negocios TI se define como un conjunto de tareas que una empresa debe realizar en caso de fallas en sus sistemas que impidan el normal funcionamiento de los servicios TI, el fin es recuperar en el menor tiempo posible las operaciones de la organización.

Los objetivos de dicho plan son proteger la información de la organización, además del negocio e imagen de la misma; identificar los puntos débiles de TI, analizar las infraestructuras de TI; conocer la logística y personas o proveedores involucrados en los mismos, ofrecer alternativas para los servicios críticos de la organización.

Para llevar a cabo de la mejor manera la Continuidad de Negocio de Tecnología de la Información (TI) es importante la implementación de estas 3 fases:

1. **Levantamiento inicial de TI**: En esta etapa se debe tener un conocimiento general de todos los servicios operativos involucrados, criticidad, personas involucradas. Luego se analizara cuáles son los riesgos asociados para mitigas las causas que puedan llegar a interrumpir el funcionamiento normal de Tecnología de la Información (TI).

2. **Levantamiento detallado de TI:** Se realizara un levantamiento más profundo de todo el hardware, software, personas, involucrados en la operativa diaria del centro de procesamiento de datos.

3. **Informe Final:** En la última etapa se dará un informe final explicando la situación actual, un plan de sugerencias y plan de pruebas y el recurso humano involucrado en cada actividad.

Gestión de la Continuidad del Servicio de Tecnología de la Información (TI) - ITSCM

Su objetivo principal es controlar riesgos que podrían impactar seriamente los servicios de TI. La Gestión de la Continuidad del Servicio de TI siglas en ingles (ITSCM) se ocupa de que el proveedor de servicios de TI siempre pueda proveer un mínimo nivel del servicio propuesto reduciendo el riesgo de eventos desastrosos hasta niveles aceptables y planificando la recuperación de servicios de TI. La ITSCM debe diseñarse para que apoye la gestión de la continuidad del negocio.

- **Definición de Proceso:**

El proceso ITIL (La Biblioteca de Infraestructura de Tecnologías de Información) V3 Gestión de la Continuidad del Servicio de TI (ITSCM) abarca los siguientes subprocesos:

Diseño del Servicio para Continuidad

Objetivo Principal: Diseñar mecanismos y procedimientos de continuidad adecuados y justificables en términos de costos para cumplir con los objetivos propuestos en el renglón de continuidad en la empresa. Esto incluye el diseño de planes de recuperación y medidas de reducción de riesgo.

Soporte a ITSCM

Objetivo Principal: Asegurar que todo el personal de Tecnología de la Información (TI) a cargo de prevenir y contrarrestar desastres tengan pleno conocimiento de sus responsabilidades, y proveerles toda la información relevante en casos de desastre.

Adiestramiento y Pruebas en ITSCM

Objetivo Principal: Asegurar que todas las medidas preventivas y mecanismos de recuperación en caso de eventos desastrosos sean objeto de pruebas frecuentes.

Revisión de ITSCM

Objetivo Principal: Revisar si las medidas de prevención de desastres son cónsonas con las percepciones de riesgo en la empresa, y verificar que las medidas y procedimientos de continuidad sean sometidas a prueba y reciban mantenimiento frecuente.

Términos ITIL

- **Estrategia de Continuidad del Negocio**

Es una guía general de acercamiento para asegurar la continuidad de funciones vitales para la empresa en caso de eventos de desastre. La Estrategia de Continuidad del Negocio es preparada por la empresa y sirve de punto de partida para la producción de la Estrategia de Continuidad de Servicios de Tecnología de la Información (TI).

Guía para Casos de Desastre

Es una guía producida por la Gestión de la Continuidad de los Servicios de Tecnología de la información (TI), con instrucciones detalladas sobre cuándo y cómo recurrir al procedimiento para contrarrestar un desastre.

Más importante aún, la guía establece los primeros pasos que debe tomar el Service Desk tras sospechar o enterarse que ha ocurrido un desastre.

Índice de Datos Relevantes en Casos de Desastre

Es un catálogo con toda la información relevante en casos de desastre. Este documento es actualizado y puesto a circular por la Gestión de la Continuidad de los Servicios de TI entre todo el personal de Tecnología de la Información (TI) a cargo de contrarrestar desastres.

Informe de Continuidad de Servicios de Tecnología de la información (TI)

Se crea cada cierto tiempo y provee información relacionada con la prevención de desastres a otros procesos de Gestión de Servicios y la dirección de Tecnología de la Información (TI).

Estrategia de Continuidad de Servicios de Tecnología de la información (TI)

Contiene una guía de acercamiento para asegurar la continuidad de los servicios de TI en casos de desastre. Incluye una lista de Funciones Empresariales Vitales y opciones de aplicaciones para la reducción de riesgo (recuperación). La Estrategia de Continuidad de Servicios de TI debe basarse en una Estrategia de Continuidad del Negocio.

2.10 Plan de recuperación de Desastres, siglas en inglés (DRP)

El plan de recuperación de desastres por sus siglas en inglés (DRP) no es más que un proceso documentado o conjunto de procedimientos que se emplean para recuperar y proteger la infraestructura tecnológica de una empresa, tales como datos, hardware o software crítico para que un negocio pueda comenzar de nuevo sus operaciones en caso de un desastre, ya sea natural o causado por humanos. Dada a la creciente dependencia de las empresas a la tecnología de la información a la hora de dirigir sus operaciones y toma de decisiones, un plan de recuperación de desastres cobran cada día más relevancia, por lo tanto, es una herramienta indispensable que toda empresa debe poseer.

Según IBM Se cree que algunas empresas gastan hasta el 25 % de su presupuesto en proyectos de recuperación de desastre, sin embargo, esto lo hacen para evitar pérdidas más grandes. De las empresas que han tenido una pérdida principal de registros automatizados, el 43 % nunca vuelve a abrir, el 51 % cierra en menos de dos años y sólo el 6 % sobrevivirá a largo plazo.

2.11 Plan de Continuidad de Negocios, siglas en inglés (BCP)

Razones por la cual recurrir a un, sistema de recuperación de desastres siglas in en inglés,(DRP)

Existen diferentes riesgos que pueden impactar negativamente las operaciones normales de una organización. Una evaluación de riesgo debería ser realizada para ver que constituye el desastre y a que riesgos es susceptible una empresa específica, incluyendo:

- Virus, amenazas y ataques informáticos.
- Catástrofes.
- Fuego.
- Fallos en el suministro eléctrico.
- Ataques terroristas.
- Sistema y/o fallos del equipo.
- Error humano.
- Cuestiones legales.

Objetivos

La dirección de la empresa debe tomar la decisión de emprender el plan como un proyecto para así satisfacer los siguientes objetivos:

- Determinar la vulnerabilidad a las interrupciones del servicio importantes en el centro de datos e instalaciones de negocios y definir las medidas preventivas que se pueden tomar para reducir al mínimo la probabilidad y el impacto de las interrupciones.
- Identificar y analizar el coste, servicio, la imagen pública y otras consecuencias de las interrupciones prolongadas del servicio en el centro de datos y otras instalaciones empresariales.
- Determinar las necesidades de recuperación y los recursos necesarios.
- Identificar las alternativas y seleccionar los métodos más rentables para proporcionar la función de las operaciones de copia de seguridad y la restauración de un servicio a tiempo.
- Desarrollar e implementar planes de contingencia que se ocupan de las necesidades para el centro de datos y otros servicios empresariales.

La suma de todos esos objetivos individuales nos ayudará a completar el objetivo principal de un DRP que no es más que la de reducir al mínimo el tiempo de inactividad tecnológica y la pérdida de datos con una recuperación ordenada después de un desastre.

Beneficios:

Hay grandes beneficios que se pueden obtener a partir de la elaboración de un plan de recuperación de desastres. Algunos de estos son:

- La capacidad de proteger los sistemas críticos para la empresa.
- Reducción de pérdidas tras un incidente.
- Garantizar la fiabilidad de los sistemas de reserva.
- Proporcionar un sentido de seguridad.
- Minimizar el riesgo de retrasos.
- Proporcionar un estándar para probar el plan.
- Minimizar la toma de decisiones en caso de desastre.
- La reducción de las posibles responsabilidades legales.
- Mejora de la eficiencia general de la organización y la identificación de la relación de bienes y recursos humanos y financieros para los servicios críticos.

2.12 Análisis de Impacto del Negocio, siglas en inglés (BIA)

El plan de continuidad de negocios por sus siglas en inglés (BCP) es un plan logístico para la práctica de cómo una organización debe recuperar y restaurar sus funciones críticas, parciales o totalmente interrumpidas dentro de un tiempo predeterminado, después de una interrupción no deseada o desastre. Este plan se compone de varias fases que comienzan con un análisis de los procesos que componen la organización. Este análisis servirá para priorizar qué procesos son

críticos para el negocio y establecer una política de recuperación ante un desastre. Por cada proceso se identifican los impactos potenciales que amenazan la organización, estableciendo un plan que permita continuar con la actividad empresarial en caso de una interrupción.

Cualquier empresa de cualquier tamaño debería planificar la mitigación del daño producido por un desastre disponiendo de un plan de continuidad del negocio.
La responsabilidad del establecimiento de un plan de continuidad de negocio (BCP) es de la alta gerencia. El plan deberá tratar todas las funciones y recursos humanos/materiales requeridos para que la organización sea viable después de que ocurra una interrupción, minimizando de esta forma sus consecuencias. Lo que reducirá el número y la magnitud de las decisiones que se toman durante un período en que los errores pueden resultar mayores.

El BCP abarca los siguientes planes:

- Plan de reanudación de negocios
- Plan de emergencia del personal
- Plan de continuidad de operaciones
- Plan de manejo de incidentes
- Plan de recuperación de desastres

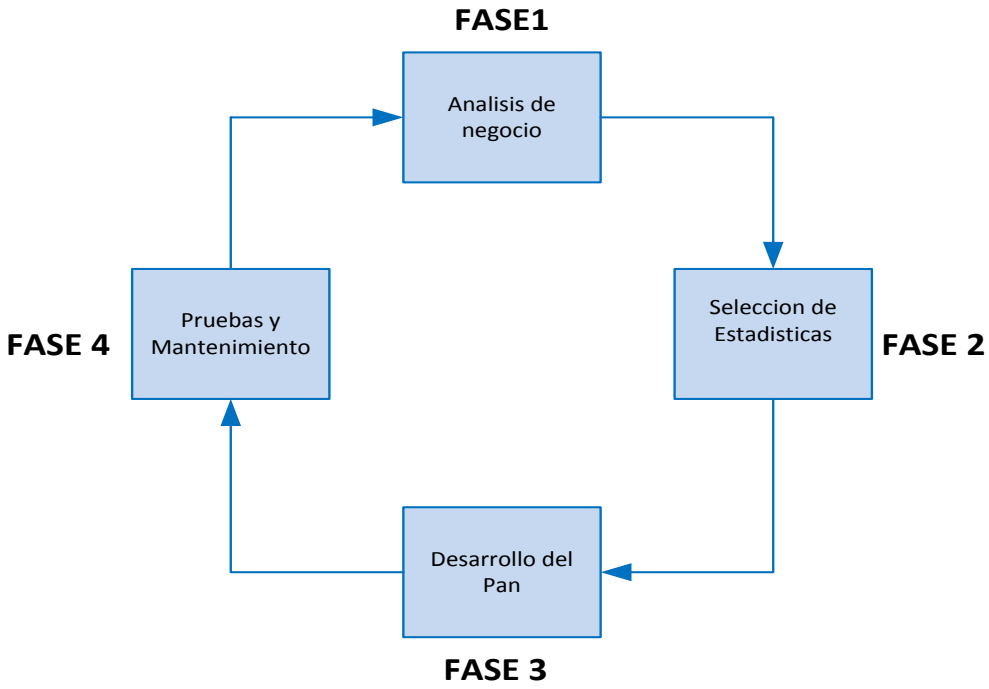


Grafico 12. Fases Plan de Continuidad de Negocios: Fuente propia

Fases del Plan de Continuidad de Negocios (BCP)

Este plan consta con un ciclo de vida el cual está compuesto por 4 grandes fases que son:

1. Análisis del Negocio y la Evaluación de Riesgos: Trata de obtener un conocimientos de cuáles son los objetivos del negocio y los procesos que la compañía considera como críticos para su funcionamiento. Ya luego que se identifican esos procesos, se analiza cuáles son los riegos analizados a dichos procesos y se identifican cuáles son las causas potenciales que pueden llegar a interrumpir un negocio.

2. Definición de Estrategias: valorar las diferentes alternativas y estrategias de respaldo en función de los resultados obtenidos en la fase anterior, para seleccionar la más adecuada a las necesidades de la compañía y corregir las vulnerabilidades en los procesos críticos del negocio detectada en el Análisis de riesgo.

3. Desarrollo del Plan: Una vez que ya son identificadas las estrategias de respaldo hay que desarrollarla e implementarla dentro del negocio. Esto incluye el desarrollo de los procedimientos y planes de actuación de las distintas aéreas y equipos y cuales intervienen en cada plan.

4. Pruebas y mantenimiento: Se prueba que el plan de continuidad de negocios realmente funciona y es efectivo. También se define los procedimientos de mantenimiento del plan.

Objetivos

El objetivo principal del plan de continuidad de negocios (BPC) no es más que disminuir y evitar las interrupciones del negocio que tienen un impacto sobre la efectiva ejecución de los procesos críticos de una organización.

Beneficios

Entre los beneficios que ofrece un BCP tanto para el negocio como para el área de Tecnología de la Información (TI) podemos mencionar los siguientes:

- Identifica los diversos eventos que podrían impactar sobre la continuidad de las operaciones y su impacto financiero, humano y de reputación sobre la organización.
- Obliga a conocer los tiempos críticos de recuperación para volver a la situación anterior al desastre sin comprometer al negocio.
- Previene o minimiza las pérdidas para el negocio en caso de desastre.
- Clasifica los activos para priorizar su protección en caso de desastre.
- Aporta una ventaja competitiva frente a la competencia.

2.13 Análisis de Impacto del Negocio (BIA).

El análisis de impacto al negocio, siglas en inglés (BIA) tiene como propósito determinar y entender que procesos son esenciales para la continuidad de las operaciones y calcular su posible impacto.

Con este informe la compañía tiene la capacidad de clasificar los procesos de negocio en función de su criticidad y lo que es más importante: establecer la prioridad de recuperación (o su orden secuencial).

También este análisis permite cuantificar las pérdidas después de una interrupción con el objetivo de que la organización pueda tomar decisiones sobre la tecnología para proteger sus activos clave en función del máximo tiempo posible de inactividad. Al analizar los costes que supondría una interrupción del

negocio frente a los costes que supondrían el establecimiento de estrategias de recuperación, la organización podría encontrar el punto en el que ambos costes se minimizan.

Propósito de un BIA

- Proporcionar al negocio las bases para un plan de continuidad de negocios
- Proporcionar a la dirección un hallazgos informativos, entendibles y objetivo para que pueda dar los lineamientos para el desarrollo del programa de continuidad de negocios
- Comunicar las vulnerabilidades inherentes de las unidades del negocio, sistemas y procesos del negocio que forma la empresa.
- Identificar que procesos y activos del negocio requieren el más alto nivel de protección
- Proporcionar información que ayude a la identificación de estrategias y alternativas
- Proporcionar datos financieros para apoyar la selección de niveles adecuados de inversión para la protección
- Establecer los objetivos de recuperación y la línea de tiempo.

Dentro del BIA podemos identificar las siguientes actividades:

- Obtención de la relación de procesos: En esta actividad se deben definir los procesos de negocio que se realizan en la empresa.

- Obtención de la relación de aplicaciones: Se identifica la relación de las aplicaciones que soportan los procesos de la compañía.
- Relación de departamentos y usuarios: Se identifican los departamentos que hay en la empresa, el nombre de las personas que lo componen e intervienen en los procesos.
- Identificar procesos críticos: En esta actividad hay que darle dos valoraciones a los procesos, valoración cualitativa y valoración cuantitativa. Importantizar los procesos cuya ausencia tendría un impacto alto en la actividad de la compañía (valoración cualitativa) e identificar las pérdidas económicas por periodo debido a la ausencia de los procesos (valoración cualitativa).
- Calcular el RTO (tiempo de recuperación objetivo), RPO (punto de recuperación objetivo) y MTD (Máximo tiempo tolerable fuera de servicio): Una vez definidos los procesos críticos del sistema, se debe proceder a realizar un análisis de impacto identificando qué sucede si uno de estos procesos permanece por fuera una determinada cantidad de tiempo. Se busca de esta manera estimar el tiempo máximo que estando el sistema interrumpido, pondría en riesgo la continuidad del negocio.

2.14 Riesgo y Cumplimiento

La computación en la nube está cargada de riesgos de seguridad, y muchos clientes inteligentes les hacen preguntas a los proveedores de nubes y

consideran la realización de una evaluación de seguridad antes de comprometerse a adoptar la solución en la nube según dice la firma de consultores de tecnología Gartner en su informe titulado "Evaluación de los riesgos de seguridad del cloud computing". Si ya estamos encaminados a la nube, para realizar una correcta gestión de riesgo durante el proceso de migración es necesario identificar los principales eventos asociados al proceso de migración que puedan afectar a la productividad de la organización, es decir, se deben identificar esos riesgos que puedan afectar directamente los procesos, sistemas y personas de la organización, y desarrollar marcos de gestión de los riegos.

AMENAZA	EXPLICACION
Robo de Datos	Que los datos del cliente sean accedidos por terceros no autorizados
Perdida de Datos	Que los datos del clinte se elimeninen y se pierdan
Secuestro de cuenta	Que un tercero no autorizado tenga acceso a la cuetant del cliente para utilizar los recursos contratados con malas intensiones
Apis Inseguras	Que las interfaces de acceso a los recursos contratados sean vulnerables a diferentes tipos de ataques
Denegacion de Servicio	Que el cliente no pueda acceder a los recursos contratados los servicios
Atacantes Internos	Que empleados actuales o pasados del cliente o del proveedor aprovechen sus privilegios con mala intensiones
Abuso de Servicios Cloud	En este caso la amaneza es para el proveedor , que el cliente haga un mal uso de los servicios contratados
Analisis Insuficientes del Proveedor	Que el cliente no analice al proveedor lo suficiente antes de establecer con el una relacion contractual
Problemas del Multi-Tenacy	Que la comparticion de los recursos físico por parte de diferentes clientes les haga vulnerables a diferentes tipos de ataques que se apoyen en la tecnologia de virtualización

Tabla 01. Las 9 amenazas más importantes que perciben cuando utilizan entornos en la nube: Fuente propia basada en el libro Cloud Computing, Tecnología y Negocios

En el informe Evaluación de los riesgos de seguridad de la computación en la nube (cloud computing) desarrollado por Gartner los principales riesgo, recomendaciones y buenas prácticas se resumen en:

Accesos de Usuarios con Privilegios: Esas informaciones sensibles fuera de la empresa conlleva un riesgo inherente, ya que es posible que estos servicios externos sorteen los controles físicos, lógicos humanos siendo, por este motivo necesario conocer quién maneja dichos datos. Por tanto, es de carácter obligatorio consensuar con el proveedor los usuarios que tenga acceso a esos datos, lo que reduce el riesgo de que haya usuarios privilegiados que no deberían tener acceso a ellos.

Cumplimiento Normativo: Los clientes son en última instancia responsables de la seguridad e integridad de sus datos, aunque estos se encuentren fuera de las instalaciones y gestionados por un proveedor de servicios de la nube. Los prestadores de servicios tradicionales se hallan sujetos a auditorías externas y certificaciones de seguridad, por lo tanto los proveedores de servicios en la nube también deben acogerse a este tipo de prácticas. Si se negasen a este tipo de auditorías no se les debería confiar los datos sensibles de la empresa.

Localización de los Datos: Al usar ambientes en la nube no se sabe de forma exacta en que país están alojados. Se debe consultar con los proveedores cuál es el marco regulatorio aplicable al almacenamiento y procesado de datos,

siendo una buena práctica cerrar un acuerdo con el proveedor para que el tratamiento de los datos se subyugue al marco legal del país del suscriptor del servicio.

Aislamiento de Datos: El entorno en nube conlleva que los datos compartan infraestructura con datos de otros clientes. El cifrado de los datos es una buena práctica, pero el problema es cómo aislar los datos cuando se encuentran en reposo ya que el cifrado, cuando no se hace uso de los datos, puede resultar una operación costosa. El prestador del servicio debe garantizar que los datos en reposo estarán correctamente aislados y que los procedimientos de cifrado de la información se realizarán por personal experimentado, ya que el cifrado de los datos mal realizado también puede producir problemas con la disponibilidad de los datos o incluso la pérdida de los mismos.

Recuperación: Los proveedores deben tener una política de recuperación de datos en caso de la ocurrencia de un desastre. Se debe exigir a los proveedores los datos sobre la viabilidad de una recuperación completa y el tiempo que podría tardar.

Soporte Investigativo: La investigación de actividades ilegales en entornos de la nube puede ser una actividad casi imposible, porque los datos y registros de actividad (Logs) de múltiples clientes pueden estar juntos e incluso desperdigados por una gran cantidad de equipos y centros de datos. Lo

recomendable será que el proveedor garantice que los logs y los datos de los incidentes se gestionan de una forma centralizada.

Viabilidad a Largo Plazo: En un entorno basado en la nube lo ideal sería que el proveedor permanezca en el mercado dando un servicio de calidad y con disponibilidad completa, pero en un mercado tan cambiante puede darse el caso de que dicho proveedor sea comprado por otro con mayores recursos.

El cliente debe asegurarse de que podrá recuperar sus datos aun en el caso de que el proveedor sea comprado o bien contemplar la posibilidad de que los datos puedan ser migrados a la nueva infraestructura.

El Instituto Nacional de Normas y Tecnología, siglas en inglés (NIST) publico recientemente un borrador de unas de sus guías "Directrices sobre seguridad y privacidad en la computación en la nube publica" en los que propone unos refuerzos de seguridad, resumiremos la parte de cumplimiento.

Cumplimiento

El cumplimiento obliga a la conformidad con especificaciones estándares, normas o leyes establecidas. La legislación y normativa relativa a privacidad y seguridad varía mucho según los países con diferencias a nivel nacional, regional o local haciendo muy complicado el cumplimiento en la nube.

Ubicación de Datos

Entre los principales problemas de los servicios en la nube se encuentra la ausencia de información acerca de cómo se ha implantado la infraestructura, por lo que el usuario no tiene prácticamente información de cómo y dónde son almacenados los datos ni de cómo son protegidos los mismos.

La posesión de certificaciones de seguridad o la realización de auditorías externas por parte del proveedor mitiga, en parte el problema, pero no es una solución.

Cuando la información se mueve por distintos países, sus marcos legales y regulatorios cambian, lo que afecta la forma de manejar los datos. Esta es una de las razones de porque la principal preocupación del cumplimiento recae en conocer los limites en los que deja de aplicar la legislación de país destino de los mismos, así como la legislación en el destino supone algún riesgo o beneficio adicional. Por lo general, aplican las salvaguardas técnicas, físicas y administrativas, como los controles de acceso.

Investigación electrónica

La investigación electrónica se ocupa de la identificación, la recolección, el procesamiento, el análisis y la producción de los documentos en la fase de descubrimiento de un procedimiento judicial.

Las organizaciones también tienen obligaciones para la preservación y la generación de los documentos, tales como cumplir con las auditorias y solicitudes de información. Estos documentos no solo incluyen correos electrónicos, también poseen metadatos.

Las capacidades de un proveedor de nube y las herramientas de investigación disponibles pueden dificultar el cumplimiento de las obligaciones de la organización.

CAPITULO III.
SISTEMA DE CONTINUIDAD DE NEGOCIO

Antes de iniciar el tema de los siguientes sistemas de continuidad de negocios debemos tener claro los conceptos, las tecnologías y herramientas que apoyan este sistema.

Continuidad de Negocios:

Es la capacidad de una organización para seguir ofreciendo productos o servicios a unos niveles redefinidos aceptables, después de un incidente disruptivo.

Propósito de alta disponibilidad como apoyo a la continuidad del negocio

El propósito de la ata disponibilidad es minimizar o mitigar el impacto del tiempo de inactividad. Una estrategia eficaz con este fin equilibra de manera óptima los procesos empresariales y los contratos de nivel de servicio (SLA).

Alta disponibilidad

La alta disponibilidad se trata de que los servicios y/o aplicaciones estén disponibles la mayor cantidad de tiempo posible para evitar pérdidas de información o inconvenientes para prestar determinado servicio. La alta disponibilidad se mide como el tiempo que el sistema (aplicaciones y/o servicios) están disponible y se representa como un porcentaje.

- **Herramientas**

  - **Clúster:**

Termino común para identificar el mecanismo de distribuir un servicio sobre un número de servidores para incrementar la tolerancia a fallas y soportar mayores cargas que las que podría soportar un servidor simple.

Los sistemas basados en clúster se implementan con el objetivo de mejorar la disponibilidad de los servicios que se ofrecen el diseño y la aplicación de un clúster de alta disponibilidad es una tarea compleja que requiere tanto de software específico como de una arquitectura.

  - **Round Robín**

Es un método para seleccionar todos los elementos en un grupo de manera equitativa y en un orden racional, normalmente comenzando por el primer elemento de la lista hasta llegar al último y empezando de nuevo desde el primer elemento.

Al mismo tiempo puede funcionar en equipos de comunicaciones un método de balanceo de tráfico basado en la jerarquía DNS existente. Esta técnica se caracteriza principalmente por su sencillez ya que no necesita el uso de ningún hardware ni software adicional.

Round Robín, que distribuye por igual las peticiones entre los servidores disponibles.

Ratio, que nos permite distribuir las peticiones de forma asimétrica entre los servidores del pool en función de los pesos asignados a cada miembro.

Replicación de Datos

Es el proceso de copiar y mantener actualizados los datos en varios nodos de Base de Datos ya sean estos persistentes o no. Éste usa un concepto donde existe un nodo amo o maestro (*master*) y otros sirvientes o esclavos (*slaves*).

Fail Over

Hace referencia a la capacidad de un sistema de acceder a la información, aun en caso de producirse algún fallo o anomalía en el sistema.

Una posibilidad es que el fallo se deba a daños físicos en uno o más componentes de hardware.

Tipos de Alta Disponibilidad

Es importante destacar que en la actualizad existen varios tipos de alta disponibilidad en esta oportunidad nos enfocaremos más bien en los conceptos de los mismos:

- **Aplicaciones**

Las aplicaciones en alta disponibilidad son aplicaciones que están optimizadas para funcionar con la tecnología de clúster basada en hardware, el software de alta disponibilidad es capaz de arrancar automáticamente los servicios que han fallado en cualquiera de las otras máquinas del clúster, incluso en la nube.

- **Base de datos**

Es un conjunto de múltiples bases de datos lógicamente relacionadas las cuales se encuentran distribuidas en diferentes espacios lógicos e interconectados por una red de comunicaciones.

- **Comunicaciones**

En equipos de comunicación con alta disponibilidad, ofrece disponibilidad en el funcionamiento de los equipos de redes tales como: Switch, Router, Balanceadores de carga y duplicación de servicios con diferentes proveedores de servicios de comunicaciones.

Muchos de los fabricantes para poder realizar esta alta disponibilidad utilizan estándares o protocolos propietarios en el caso de CISCO utiliza utilizan un protocolos VRRP (Virtual Redundancy Router Protocol) CISCO HSRP (Hot Stand-by Redundancy Protocol).

- **Seguridad**

La alta disponibilidad en los equipos de seguridad está basado en realizar una copia de la configuración de un dispositivo a otro mediante un cable punto a punto entre ellos cada vez que ocurre un cambio se sincronizan, entre los equipos de seguridad se involucran , Firewall, Prevención de Intrusos, Equipos de protección de correo, equipos para la navegación, entre otros.

- **Virtualización**

En la actualidad los sistemas o soluciones virtualizadas poseen herramienta que se anticipa a los fallos provenientes del sistema operativo de las máquinas virtuales y/o los fallos de hardware en el servidor que alberga dichas máquinas virtuales. Si el daño se presenta en el sistema operativo una máquina virtual, ésta puede ser reiniciada en el mismo servidor, pero si el daño es en el hardware del servidor físico que alberga varias máquinas virtuales, en esta situación el equipo que está disponible pasa o activa las máquinas virtuales que están ya replicadas en sus sistema de alta disponibilidad.

3.1 Sistema de Continuidad Basado en Servicio

El software es el nivel más alto que ofrece aplicaciones como servicio bajo demanda, de manera que instancia del software se ejecutan en la infraestructura del proveedor para ofrecer el servicio a los clientes a través de internet.

Características

- El sistema de alta disponibilidad está garantizado 99.999 %. Fuente: Microsoft
- La inversión en seguridad y los datos es 100% responsable del proveedor de servicio
- Estos sistemas operan 24x7 y replicados en diferentes Datacenter
- El licenciamientos de estos servicios es por renta, mensual, o anual o demanda
- Dependiendo del tipo de servicio puede ser compartido o privado
- Totalmente escalable.

3.2 Sistema de Continuidad Basado en Aplicaciones

Las aplicaciones de continuidad de negocios están basadas en plataforma como servicio (Paas) en la encapsulación del entorno de desarrollo ofreciéndolo como servicio.

Aquí el servicio es proveer soporte a la creación de las aplicaciones, no las aplicaciones en sí mismas. PassS genera todas las facilidades requeridas para soportar el ciclo completo de construir y poner en funcionamiento las aplicaciones basadas en internet en general no se requiere descargar software o instalaciones especiales para su desarrollo.

Características

- Reduce el tiempo de implementación puesto que no se requiere instalar entornos de desarrollo e implementación, puesto que no se requiere instalar entornos para este propósito.
- Facilita las actualizaciones de versiones de forma centralizada.
- Ahorra inversión en activos.
- Ahorro en contracción en especialistas de base de datos y de aplicaciones.

3.3 Sistema de Continuidad Basado en la Recuperación de Desastres

Plan continuidad de negocios es un proceso diseñado para reducir el riesgo del negocio de la organización que surja de una interrupción no esperada de las funciones/operaciones críticas (manuales o automáticas) necesarias para la supervivencia de la misma. Esto incluye recursos humanos/materiales que soportan estas funciones/operaciones críticas y garantía de la continuidad de por lo menos el nivel mínimo de los servicios necesarios para al menos las operaciones críticas.

Continuidad de negocios enfocado a los sistemas de información de Tecnología de la información (TI)

El plan de continuidad del negocio del SI debe también estar alineado con la estrategia de la organización. De ese modo, la clasificación con respecto a la

criticidad de los diversos sistemas de aplicación desplegados en la organización depende de la naturaleza del negocio así como también del valor de cada aplicación del negocio.

Un plan de continuidad del negocio de SI es mucho más que sólo un plan para los sistemas de información. Un BCP identifica lo que el negocio hará en el caso de un desastre. Un subcomponente del plan de continuidad del negocio es el plan de recuperación ante desastres de TI. Éste, típicamente detalla el proceso que el personal de TI utilizará para restablecer los sistemas de cómputo.

En los sistemas de recuperación de desastres existen dos aspectos fundamentales que con:

- **El Punto Objetivo de Recuperación, siglas en inglés (RPO)**

Cuantifica efectivamente la cantidad permitida de pérdida de datos en el caso de interrupción. Es casi imposible recuperar la totalidad de los datos. Incluso después de ingresar los datos faltantes, algunos todavía se perderán y a ellos se hace referencia como datos huérfanos.

- **El Tiempo Objetivo de Recuperación, siglas en inglés(RTO)**

Se determina sobre la base del tiempo de inactividad aceptable en caso de una interrupción de operaciones. Ello indica el punto más anticipado en el tiempo en el que las operaciones de negocio deben retomarse después del desastre.

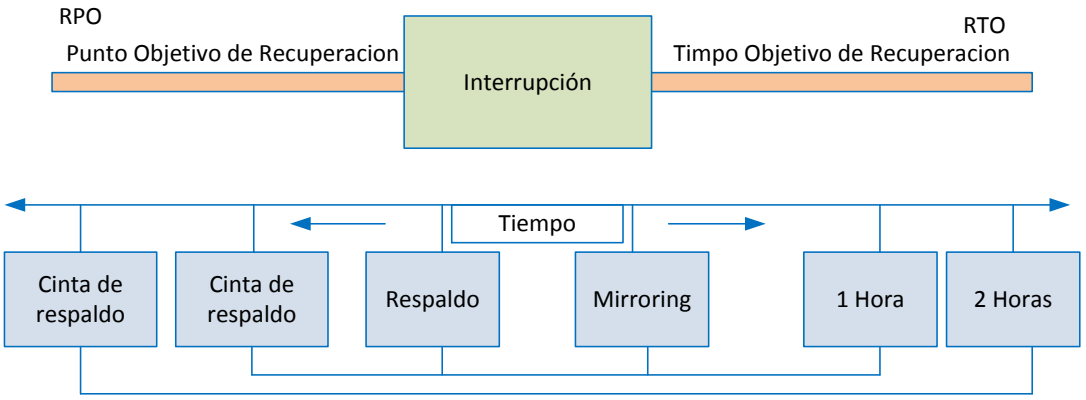


Grafico 13. Diagrama de RPO y RTO. Fuente Propia basada en ORACLE

Existen parámetros que son importantes para definir las estrategias de recuperación de desastres que son las siguientes:

Ventana de Interrupción: El tiempo que una organización puede esperar, desde el punto de falla, hasta la restauración de servicios/aplicaciones críticas. Después de ese tiempo, las pérdidas progresivas causadas por la interrupción no son aceptables

Objetivo de prestación de servicios: El nivel de servicios a proveer durante el modo de proceso alterno, hasta que se restaure la situación normal. Esto está directamente relacionado con las necesidades del negocio

Cortes máximos tolerables: El tiempo máximo que la organización puede soportar procesar en modo alterno.

Alternativas de Recuperación

Las interrupciones más prolongadas y más costosas, en particular los desastres que afectan la instalación física primaria, requieren alternativas de recuperación en un sitio distinto a la ubicación primaria (offsite). Los tipos de instalaciones de respaldo de hardware en sitio alternativo que existen son:

- **Hot Sites:** Se configuran totalmente y están listos para operar dentro de varias horas. El equipo, red y software del sistema deben ser compatibles con la instalación primaria que está siendo respaldada. Las únicas necesidades adicionales son personal, programas, archivos de datos y documentación.

El hot site está destinado para operaciones de emergencia durante un período limitado de tiempo y no para uso prolongado

- **Warm Sites:** Están parcialmente configurados, por lo general con conexiones de red y equipo periférico seleccionado, como por ejemplo, unidades de discos y otros controladores, pero sin la computadora principal. Algunas veces un warm site está equipado con una CPU menos potente que la que se usa generalmente.

Otra opción existente en el mercado es la de **acuerdo recíproco** con otras organizaciones: Este es un método usado con menos frecuencia entre dos o más organizaciones con equipos o aplicaciones similares. Bajo el acuerdo típico,

los participantes prometen proveerse mutuamente tiempos de computadoras cuando surja una emergencia

En la actualidad existen otras opciones de alternativas basados en ambientes sincronizados en la nube, en la cual puede ser privado o compartido según en el requerimiento de la empresa y el enfoque del negocio.

3.4 Sistema de Continuidad de Respaldo Basado en la Nube

Continuidad de respaldo basado en la nube están enfocados en realizar copias de información o (Backup de forma automatizada o manual, en la actualizad existen empresas que ofrecen este servicio incluso aplicaciones que tienen esta opción como valor agregado.

El respaldo es fundamentalmente para garantizar la recuperación de información esencial en el caso de daño, o perdida de datos desastres. Asimismo, la manera en que se realizan las operaciones de respaldo (Las personas, los procesos y la infraestructura) puede afectar iniciativas clave del negocio.

Puede acelerar o desacelerar el ritmo con que se implementan nuevas aplicaciones o se extiende la virtualización en la organización y puede mejorar u obstaculizar los ciclos des desarrollo de los productos, los esfuerzo de expansión global o el servicio al cliente.

Envío de backups por Internet para almacenarlos en la nube cuenta con la ventaja de la elasticidad de la capacidad y los gastos operativos típicos de los servicios en la nube. También puede simplificar la infraestructura propia, dado que ya no es necesario proporcionar y administrar el almacenamiento (por ejemplo, con cintas que se deben rotar, enviar fuera del sitio, etc.). Estos servicios ahorran costos inmediatos en nuestro país la Super Intendencia de Banco ya existe que exista una copia del backup de las operaciones diarias fuera del datacenter principal.

Empresa como Oracle ofrece este servicio en integrada a su plataforma, como se puede observar en el grafico 14.

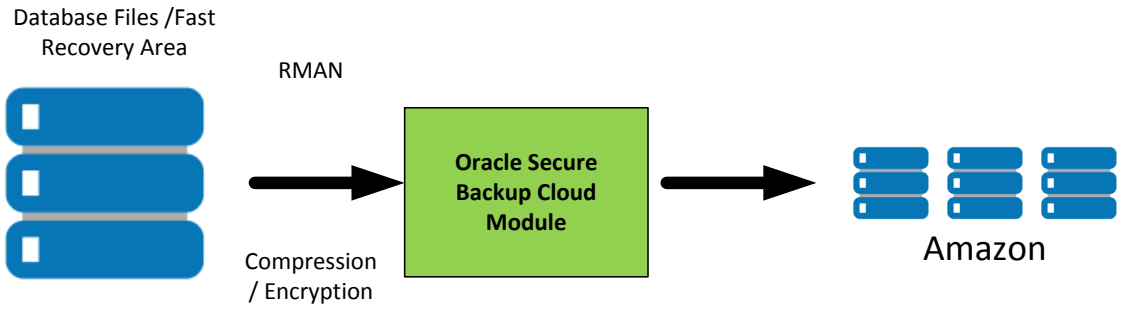


Grafico 14. Backup de Base de Datos Fuera del Sitio en la Nube.
Fuente Propia basada en ORACLE

Beneficios:

- **Accesibilidad Permanente:** Los administradores pueden comenzar con las operaciones de restauración como si estuviera almacenado localmente.
- **Alta Confiabilidad:** las nubes de almacenamiento funcionan con discos y, por eso, son esencialmente más confiables que las cintas. Asimismo, los

proveedores de la nube generalmente mantienen varias copias redundantes de los datos por razones de disponibilidad y escalabilidad

- **Escalamiento Ilimitado Sin Gastos Iniciales de Capital:** la nube ofrece una capacidad Prácticamente ilimitada sin gastos iniciales de capital. Por consiguiente, los usuarios no deben Preocuparse por el aprovisionamiento de cintas adecuadas o de almacenamiento local para conservar los datos de backup que necesitan.

La nube cuenta con un escalamiento perfecto, y los Administradores pagan sólo por lo que utilizan y cuando lo utilizan.

- **Costos Reducidos de Backup en Cinta y Almacenamiento Fuera del Sitio:** el hecho de que el backup en la nube reduzca o elimine la necesidad de cintas puede originar ahorros importantes en los costos de las licencias y el soporte de software de backup en cinta, y del almacenamiento de cintas fuera del sitio.

- **Aprovisionamiento Sencillo de Entornos de Prueba y Desarrollo:** dado que se puede acceder a los backups en la nube desde cualquier sitio a través de Internet, pueden utilizarse a fin de clonar bases de datos rápidamente para crear entornos de prueba, desarrollo y control de calidad a medida

3.5 Sistema de Continuidad de Respaldo Basado en Almacenaje

Aunque el concepto de almacenamiento en la nube puede resultar muy novedoso, la verdad es que lo llevamos usando muchos años. La nube se está convirtiendo en una de las principales alternativas para que la empresas almacenen s información.

La principal ventaja de los sistemas de gestión de archivos en la nube es que se pueda acceder a ellos desde cualquier dispositivo con una conexión a internet. Además de que todo se hace de una manera segura e independiente de la plataforma o sistema operativo que se utilice.

Actualmente, existen muchos servicios que ofrecen almacenamiento de información en la nube el cual incluye variedad de prestaciones técnicas con costo asumibles, a veces incluso gratuitos tales como Drobox, Google, Skydrive para el segmento corporativos empresas como rackspace ya está ofreciendo servicios de bigdata e incluso proveen servicios a terceros para que alojen sus datos fuera de sus propios Datacenter.

La gestión de los archivos en la nube permite a las empresas:

- Almacenar y clasificar los archivos de información que la empresa necesita para su proceso de negocio
- Compartir los archivos con seguridad, confidencialidad e integridad

- Disponer de la información de la empresa desde cualquier lugar y dispositivos que tenga acceso a internet
- Controlar las diversa versiones de sus documentos, para facilitar la asignación y seguimiento de proyectos y tareas

3.6 Sistema de continuidad en servicios de seguridad

Seguridad como Servicio, siglas en inglés (SECaaS) es la provisión de servicios de seguridad desde la nube, lo que permite que algunos servicios y tecnologías que tradicionalmente solo estaban al alcance de empresas grandes, estén accesibles a Pymes y Administraciones públicas, con las mismas, o incluso a veces más necesidades en este aspecto.

La seguridad como servicio es uno de los segmentos de las soluciones basadas en la nube con más rápido crecimiento, incluso según algunos analistas superara a los segmentos IaaS, SaaS y PaaS (Infraestructura, Software o Plataforma como servicio) en breve. Por ejemplo Forrester prevé que tendrá un crecimiento del 15% en el periodo 2009-2014, dos veces el ratio de crecimiento de los otros sectores Tecnología de la información (TI); Gartner predice que el uso de servicios de seguridad basados en la nube se triplicará en algunos sectores en el 2013.En Octubre del 2011 la Alianza de Seguridad de la Nube, siglas en inglés (CSA), en su grupo de trabajo sobre SECaaS, publicó un documento que intenta clarificar los tipos de servicios de seguridad ofrecidos desde la nube.

Este tipo de servicios quedarían englobados en una de estas categorías:

- **Gestión de Identidades y Accesos:** Servicios como Web Single-Sign-On, Federación de Identidades, Gestión de Identidades, Fairma electrónica, Gestión de autorizaciones, etc. En Septiembre del 2012 se ha publicado una guía de implantación de este tipo de servicios.

- **Prevención de Perdida de Datos, siglas en inglés (DLP):** Soluciones de prevención contra la pérdida de datos.

- **Seguridad Web:** Algunos ejemplos pueden ser soluciones de Filtrado Web, Análisis de Vulnerabilidades Web, Monitorización, Anti-phising, Anti-virus.

- **Seguridad del Correo Electrónico:** Mail Relay, Anti-Spam, Antivirus /Anti-malware, DLP para correo de salida.

- **Evaluación de la Seguridad:** Auditorias de servicios Cloud, o evaluaciones de sistemas e infraestructura instalados en el cliente (on-premise) basados en estándares, como por ejemplo test de penetración (pen-testing), evaluación de la seguridad perimetral, evaluación de la seguridad del entorno virtual, etc.

- **Gestión de la Intrusión**: Detección, prevención y reacción ante eventos inusuales, incluyendo reconfiguración de la infraestructura o los sistemas en tiempo real para detener o prever una intrusión.

- **Gestión de la Información de Seguridad y Gestión de eventos (SIEM):** Servicios basado en recopilación de eventos de seguridad (log) de los diferentes elementos de la infraestructura para correlacionarlos, analizarlos y proporcionar informes en tiempo real y alertas ante incidentes de seguridad.

- **Encriptación:** Servicios de red privada virtual (VPN), encriptación de las comunicaciones, gestión de claves.

- **Continuidad de negocio y Recuperación ante desastres (Disaster Recovery):** Orientados a garantizar el negocio en caso de problemas con la infraestructura o servicios proporcionados, como por ejemplo copias de seguridad on-line desde el cloud (Cloud Backup), Data Center alternativo (Cold, Warm o Hot Site), replicación de datos, etc.

- **Seguridad de las Redes:** Orientados a implementar los controles de seguridad en la infraestructura de red, como pueden ser soluciones de Firewall, protección de denegación de servicios, siglas en inglés (DDoS), IDS/IPS, Monitorización de infraestructura.

El desarrollo cada vez mayor de este tipo de servicios por parte de fabricantes y proveedores de Servicios Cloud (CSP), unido a la necesidad de la utilización de los mismos debido a la cada vez más compleja administración de las tecnologías de seguridad por parte de las empresas, así como a su modalidad de pago por

uso (sin requerir grandes inversiones iniciales), hace que cada vez más empresas de todo tipo estén optando por ellos, y sea uno de los caminos a seguir para conseguir un nivel de riesgo aceptable en el cada vez más necesario y cambiante mundo de los negocios en Internet.

Es importante destacar que existe una certificación para la seguridad en la nube llamada certificación start basada en la norma de seguridad ISO Al igual que con todas las normas de sistemas de gestión, ISO/IEC 27001 ha sido escrita `de tal manera que se pueda aplicar a cualquier organización, grande o pequeña, en todas las industrias. Sin embargo, se considera que existen requisitos especiales específicos para computación en la nube que o bien no están cubiertos o que necesitan ser cubiertos con mayor precisión.

Desarrollado por la Cloud Security Alliance (CSA) la Matriz de Control de la Nube (CCM) une este vacío, proporcionando un conjunto adicional de controles para los proveedores de servicios en la nube.

Un acuerdo conjunto fue firmado por la CSA y BSI en agosto de 2012 para desarrollar un tercer esquema de certificación de terceros para la seguridad en la nube llamada certificación STAR. El plan incorpora los requisitos de la norma ISO 27001 y un índice de madurez para indicar cómo de bien la organización está cumpliendo con los requisitos específicos de la nube y también para

impulsar los esfuerzos de optimización mediante la auditoría de las capacidades y las complejidades de las organizaciones también.

Este nuevo esquema ayudará en la adopción de servicios en la nube por las empresas mediante la promoción de una mayor transparencia y permitiendo que los proveedores de servicios en la nube ofrezcan a sus grupos de interés la confianza que tienen los controles necesarios para asegurar los datos que poseen.

CAPITULO IV.
INFRAESTRUCTURA TECNOLÓGICA DE LA EMPRESA

Actualmente la operación de la EMPRESA REYES & HERMANOS en lo que respecta a la Producción, Distribución, Ventas, Cobros y Finanzas, se encuentra soportada por la infraestructura tecnológica tanto a nivel de hardware como de software. En los siguientes subcapítulos se presenta un breve resumen de esta arquitectura.

4.1 Centro de Datos (Data Center)

El Centro de Datos de la EMPRESA REYES & HERMANOS cuenta con una granja de seis servidores, destinados a brindar servicios Web, Base de Datos, Aplicaciones, Inteligencia de Negocios, Correo Electrónico y Seguridad. También cuenta con una infraestructura de red bajo un esquema de diseño de CISCO.

Las características del espacio físico del centro de datos son las siguientes:

- Temperatura entre 18 a 24 grados centígrados.
- Humedad relativa entre 15% y 60%.
- Centro de Cableado para equipos de usuario final separados del Data Center.
- Un sistema de UPS independiente donde solo se conectan los equipos del Centro de Datos.

- Diseño según la norma ANSI/TIA/EIA RS-310-D que asegura la compatibilidad con el diseño de los servidores y los equipos de comunicación.
- Un sistema de detección y extinción de incendios independiente al de las instalaciones, con una tecnología que no pone en riesgo la vida humana.
- Cuenta con un control de acceso independiente con dos niveles de acceso, uno para la zona de operación y otro para la zona de servidores.
- Un transformador independiente para los circuitos eléctricos que alimentan el Centro de Datos para supresión de picos y transientes eléctricos.
- Todos los racks están conectados a tierra a través de una malla equipotencial.
- Todos los servidores tienen fuentes de poder redundantes.
- Todos los servidores son de tipo rack
- Todos los equipos del centro de datos que soportan procesos críticos, cuentan con una garantía extendida 7x24x365 con 4 horas de tiempo respuesta en sitio.
- Los servidores y equipos de comunicación están ubicados en racks separados.
- Cuenta con una nomenclatura de cableado que permite identificar qué tipo de cable corresponde a servidores, equipos de comunicación o usuarios finales.

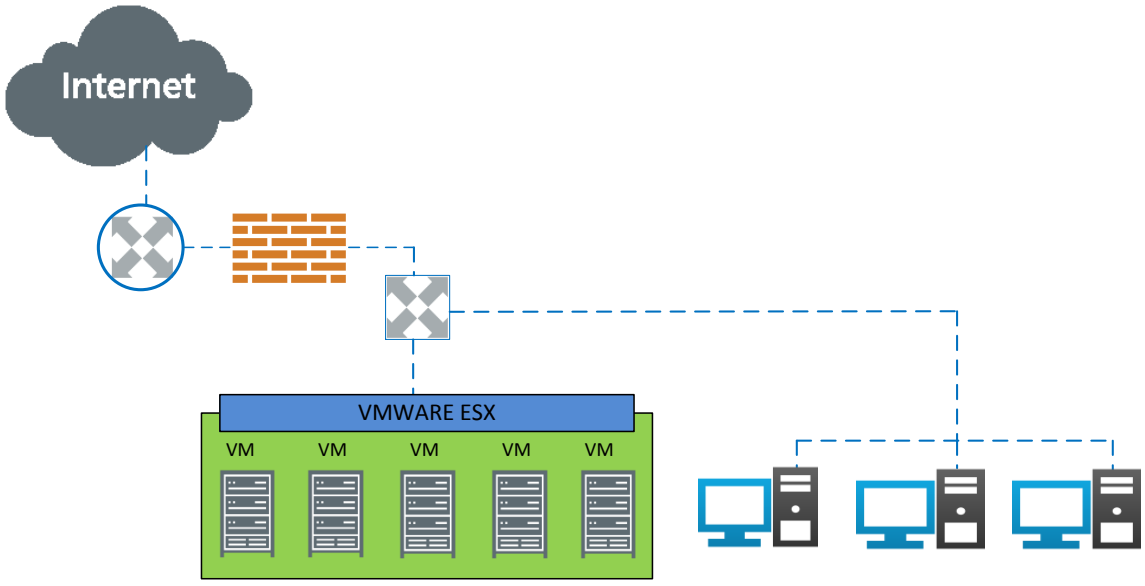


Grafico 15. Centro de Datos EMPRESA REYES & HERMANOS. Fuente propia

4.2 Infraestructura de Servidores

La granja de servidores está destinada a brindar los siguientes servicios: Web, Base de Datos, Aplicaciones, Inteligencia de Negocios, Correo Electrónico y Seguridad. Según los procesos críticos los servidores más importantes son lo que alojan el grupo de aplicaciones y base de datos.

En la tabla 01 que se muestra a continuación, se ilustran las características de estos equipos.

Nombre	Marca	RAM	Discos Duros	Espacio Utilizado en GB	Sistema Operativo	Rol del Equipo
RH001	HP DL360 G4P	2048 (2GB)	2X146=146	110	WS-2003	SERVIDOR SEGURIDAD
RH002	HP DL360 G4P	8192 (8GB)	2X146=146 1X146=146	120 120	WS-2003	SERVIDOR WEB
RH003	HP DL380 G5	3326 (3.3GB)	2X146=146	80	WS-2003	SERVIDOR BASE DE DATOS
RH004	HP DL380 G5	3326 (3.3GB)	2X146=146	105	WS-2003	SERVIDOR CORREO ELECTRONICO
RH005	HP PROLIANT ML 110	3870 (3.8GB)	2X500=500	250	WS-2003	SERVIDOR APLICACIONES, DOMINIO Y ARCHIVO
RH006	HP DL380 G5	3072 (3GB)	2X73=73	40	WS-2003	SERVIDOR BI

Tabla 02: Características Servidores EMPRESA REYES & HERMANOS. Fuente Propia

En el grafico 16 se ilustra la infraestructura de servidores que la EMPRESA REYES & HERMANOS posee actualmente.

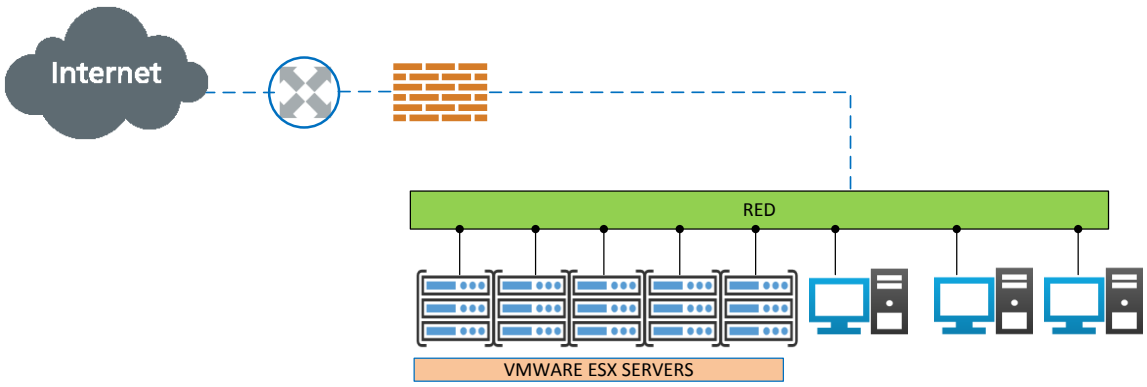


Grafico 16. Infraestructura de Servidores EMPRESA REYES & HERMANOS. Fuente Propia

4.3 Infraestructura de Comunicaciones

Los usuarios internos de la EMPRESA REYES & HERMANOS acceden a los servicios tanto de internet como a los servicios que provee el Centro de Datos, a través de la infraestructura de comunicaciones. Esta infraestructura está dividida en tres capas, Núcleo, Distribución y Acceso, diseño que se implementó buscando optimizar la velocidad de acceso a dichos servicios.

Las características de la infraestructura de cableado son las siguientes:

- El cableado estructurado esta realizado con cables, jacks y patch panels en categoría 6A de 8 hilos.
- Los cables no exceden la distancia de 90m según lo definido en el estándar TIA/EIA 568A o 568B.
- Los cables están segregados por colores y estos permiten identificar a qué tipo de equipo le provee conexión.
- Los pacth core para la conexión de equipos de usuarios finales no superan los 5m de longitud.
- Los racks de los centros de cableado son abiertos y de uso específico para equipos de comunicaciones, con organizadores verticales para el acceso de los cables y horizontales para ordenar los patch core.
- A continuación en la Tabla 02 se detallan las características de los equipos utilizados:

Capa de Red	Marca	Modelo	Cantidad Puertos	Cantidad Switches
Nucleo	CISCO	3560 - X	48	1
	CISCO	3560 - X	48	1
Distribucion	CISCO	2950 Series	24	2
	CISCO	2960 - G	24	2
Acceso	CISCO	2960 - X	48	2
	CISCO	2960 - X	48	3

Tabla 03: Características Equipos de Comunicación EMPRESA REYES & HERMANOS. Fuente Propia

En el grafico 17 se ilustra la infraestructura de comunicaciones que la EMPRESA REYES & HERMANOS posee actualmente.

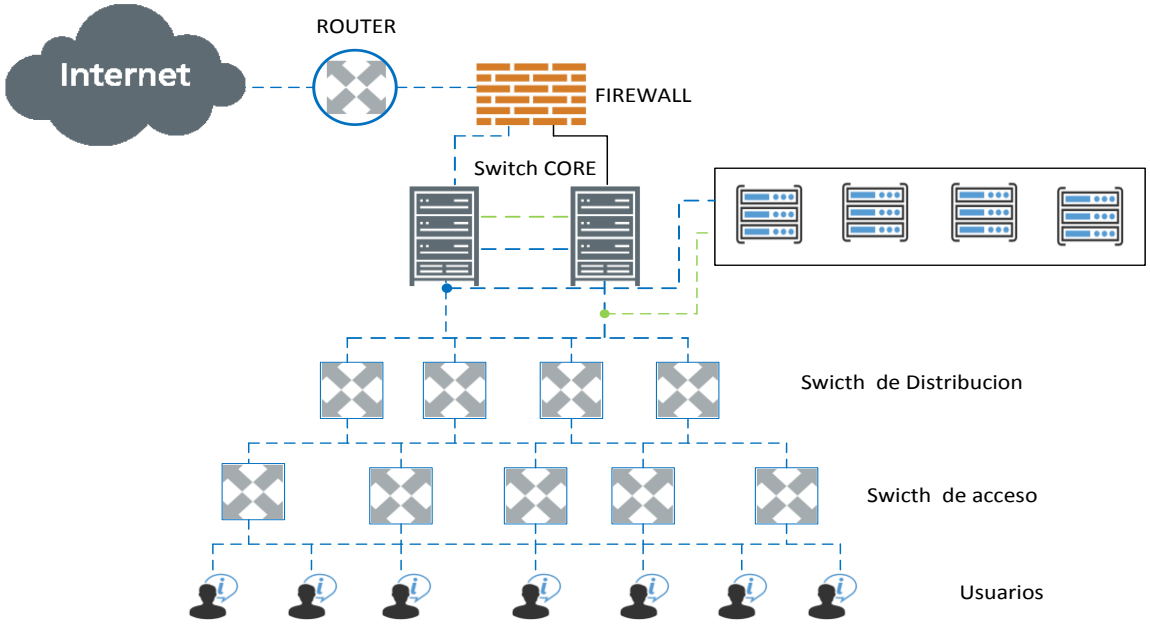


Grafico 17. Infraestructura de Comunicaciones EMPRESA REYES & HERMANOS. Fuente Propia

4.4 Sistema de Respaldo Local

Este sistema está diseñado para respaldar toda la información de la empresa en Cinta, a saber: Base de Datos del ERP, Bases de Datos Recursos Humanos, Configuración de Aplicaciones, Sistema de Archivos. Una vez las informaciones son respaldadas en las cintas, estas son trasladadas a un proveedor externo de espacio de almacenamiento físico para asegurar la información fuera de la empresa.

Las especificaciones del equipo que soporta esta operación es la siguiente:

- Tape Backup HP MSL2024 1 LTO5 Utrium 3000.

4.5 Estructura Energética

La EMPRESA REYES & HERMANOS cuenta con un UPS ubicado en el Centro de Datos. Este provee servicios para toda la infraestructura tecnológica que soporta la operación. A saber: Infraestructura de Servidores, Infraestructura de Red y a los Usuarios Internos. A continuación se muestra esta arquitectura.

Las características de la estructura energética son las siguientes:

- La autonomía del UPS central es de 20 minutos para la carga máxima soportada por el centro de datos y bajo ninguna circunstancia excede el 80% de la capacidad nominal del UPS.
- Todos los racks de equipos están conectados a energía regulada.
- Todos los racks de equipos están conectados al mismo sistema de tierra.

- La diferencia de potencial entre el neutro y la tierra del centro de datos no excede 0.7 voltios.
- El centro de datos es alimentado por dos circuitos eléctricos independientes, debido al nivel de disponibilidad requerido.
- Todos los servidores poseen fuentes de poder redundantes.

En el grafico 18 se ilustra la estructura energética que posee actualmente la EMPRESA REYES & HERMANOS.

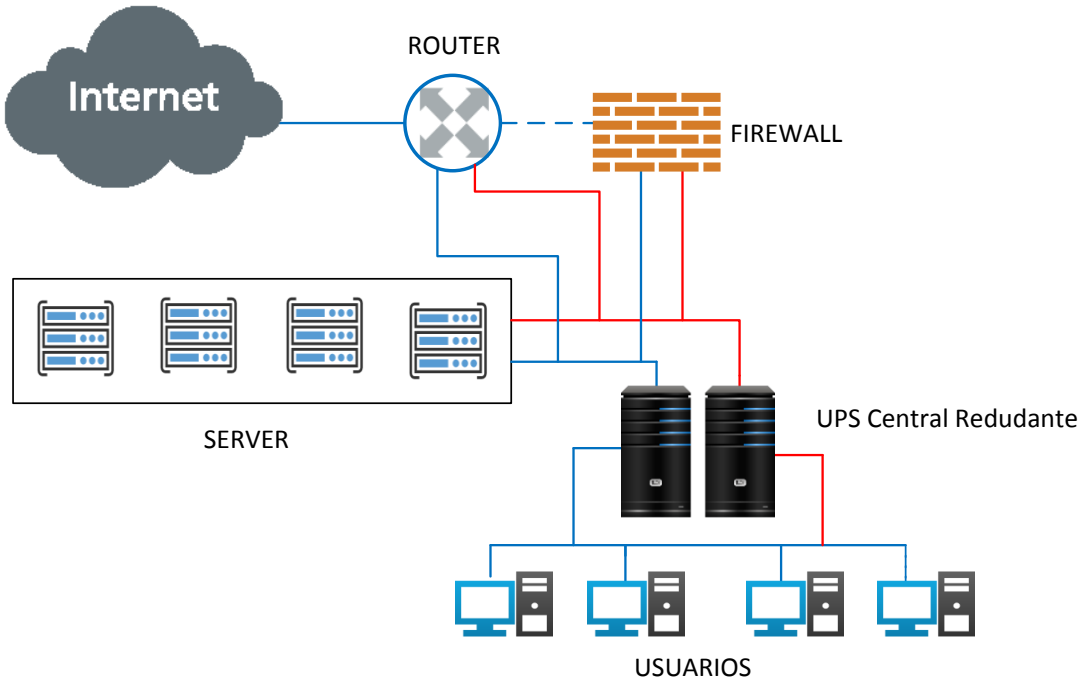


Grafico 18. Estructura Energética EMPRESA REYES & HERMANOS. Fuente Propia

CAPITULO V.
SISTEMA DE INFORMACIÓN DE LA EMPRESA

La EMPRESA REYES & HERMANOS posee un Sistema de Planificación de Recursos Empresariales (ERP: Enterprise Resource Planning) donde se centraliza los principales procesos de operación, a saber: Producción, Distribución, Ventas, Cobros y Finanzas. Este opera bajo un esquema de base de datos en UNIX.

- **El módulo de Producción:** se encarga de procesar todo lo relacionado a la materia prima integrando un sub-módulo de pesaje que permite almacenar formulas y medidas de pesaje para la elaboración del producto terminado de manera automatizada.

- **El módulo de Distribución** se encarga de administrar el almacenamiento, facturación e impresión del rutero para la distribución del producto terminado.

- **El módulo de Ventas:** se encarga de crear y administrar las rutas para la fuerza de vendedores en los diferentes canales en los que operan. Las ventas se realizan de manera manual y luego son registradas en el sistema que al mismo tiempo integra la información al módulo de Distribución para ser entregada.

- **El módulo de Créditos y Cobros:** se encarga de manejar la cartera de clientes de los diferentes canales. A qué tipo de negocio se le otorgan créditos y a que tipo deben pagar de contado. De esta manera, este módulo contribuye con el cobro oportuno de las ventas registradas en le ERP.

5.1 Sistema de Recursos Humanos

Recursos humanos posee una herramienta independiente en la que se maneja la Compensación y Bienestar de los empleados, además maneja un histórico con todas las documentaciones y novedades (hoja de vida) de cada empleado. Esta aplicación está fue adquirida a un proveedor externo y se integra con las bases de datos creadas en SQL Server 2008

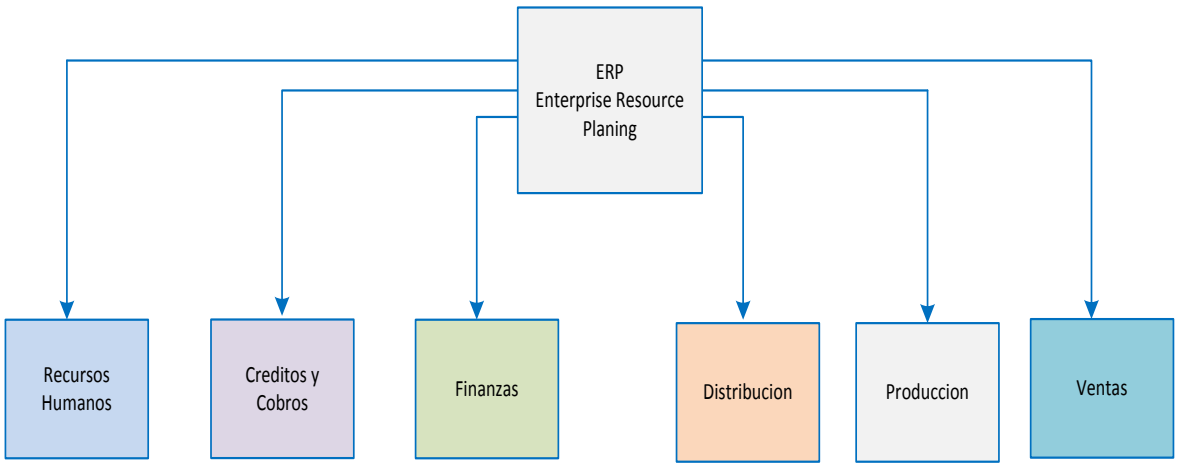


Grafico 19. Sistema de Información de la EMPRESA REYES & HERMANOS.
Fuente Propia

CAPITULO VI.
SISTEMA DE CONTINUIDAD BASADO EN LA NUBE

6.1 Sistema de Continuidad de Negocio Hibrido

La solución de continuidad de negocios de nuestro proyecto está basada en tener un ambiente de hibrido el cual consiste en combinar aplicaciones y servicios locales y replicados en una nube privada esto nos permite tener alta disponibilidad localmente como también en la nube no solamente para un caso de emergencia o de algún siniestro sino también ante cualquier eventualidad de mantenimiento programado o falla de algunos de nuestros sistemas críticos.

La nube hibrida nos brinda la posibilidad de ir migrando servicios locales a la nube de acuerdo a nuestra necesidad esto significa que podemos utilizar este servicios para momentos de alto uso.

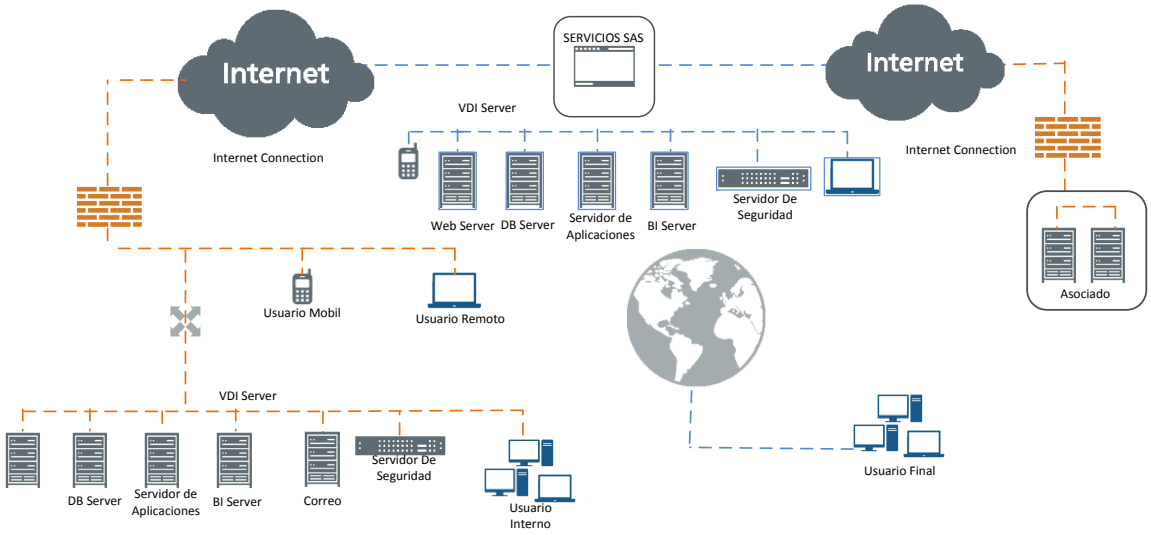


Grafico 20. Infraestructura propuesta para la EMPRESA REYES & HERMANOS. Fuente Propia

Es importante destacar que esta solución ofrecerá a los administradores de Tecnología de la Información (TI) decidir qué datos y aplicaciones estarían en la nube privada interna y que debe trasladarse a la red local. Esto es muy conveniente, ya que minimiza el exceso de capacidad de recursos. También equilibra las aplicaciones cruciales y datos dentro de la nube privada mientras se mueve pico de cargas altas tráfico y aplicaciones o datos la red local.La implementación de esta solución implica una combinación de hardware y software lo crucial de hacer que esta plataforma de continuidad de negocio basado en una ambiente hibrido es su configuración, pero los mismos se justifican debido a los siguientes beneficios:

- Integración probada de servicios de red.
- Prestación de servicios a nivel mundial.
- Implementación más rápida y con menos riesgos.
- Actualizaciones automáticas que no afectan negativamente a los recursos del Tecnología de la Información (TI).
- Contribuye al uso eficiente de la energía
- Movilidad

Basados en la combinación y buenas prácticas nos apoyamos en algunas tecnologías de empresas líderes en el mercado como Intel cual utiliza servicios de nube hibrida para uso interno utilizando Tenencia múltiple (Multitenancy), consiste en tener un ambiente separado de varias aplicaciones y servicios pero se ven como si fuese uno solo tal como se muestra en la siguiente figura:

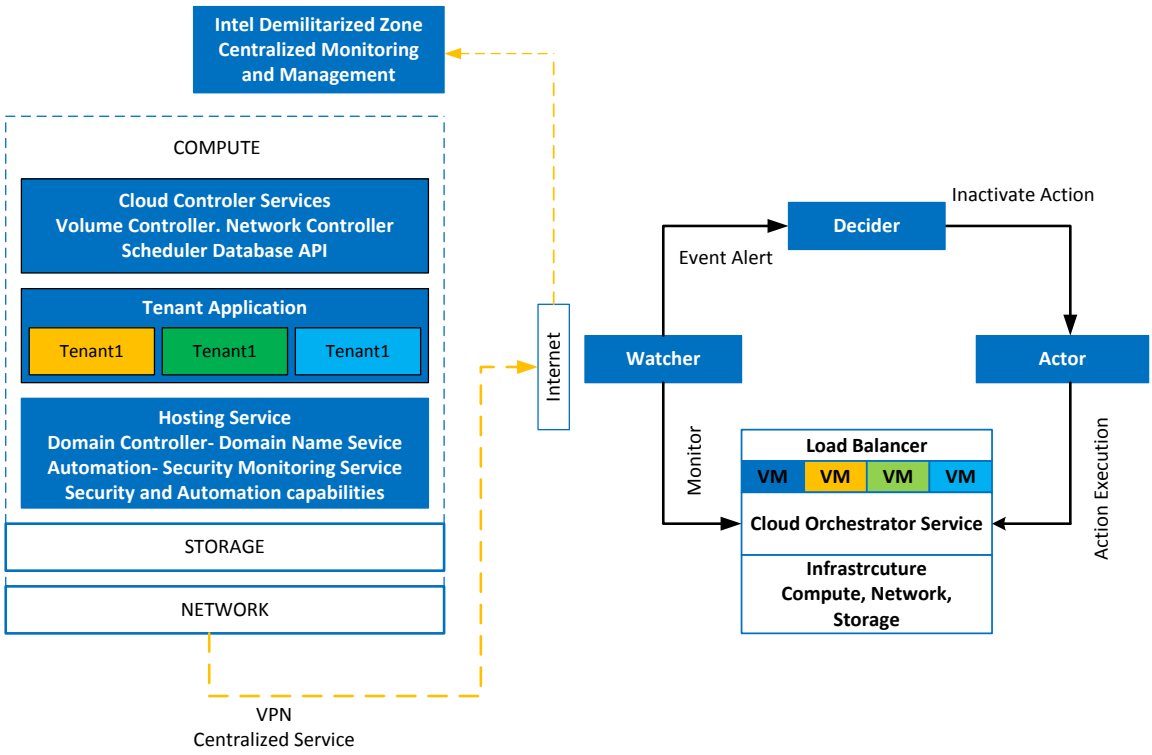


Grafico 21. Tenencia Multiple. Fuente: Intel (Developing a Highly Available, Dynamic Hybrid Cloud Environment The capabilities of open source software make common compute, network, storage, and centralized management resources available to tenant applications

Esta tecnología garantiza tener una respuesta a un evento de forma inmediata ante cualquier falla de algún componente de hardware, Software, Aplicación, Servicio, Sistema Operativo dicha estructura se encarga de monitorear cada una de los servicios en la nube que estén en una plataforma virtual.

6.2 Replicación

La replicación de datos por Internet permite a usuarios desconectados y remotos obtener acceso a los datos cuando los necesiten, por medio de una conexión a nternet.

Puede llevar a cabo la replicación de datos por Internet mediante:

- Una red Virtual Privada (VPN SITE TO SITE)
- Líneas de comunicación dedicadas
- Comunicación por servicios Web a través de internet

En la implementación la replicación de los servicios de Base de Datos, Servidor de Archivos y de correos será replicado a través de internet, algunos de estos servicios se replicaran directamente por webs-Services otros como la base de datos se utilizara una red privada virtual utilizando y aprovechando el mismo servicio de internet que posee la empresa actualmente, la cual representamos en el grafico 22.

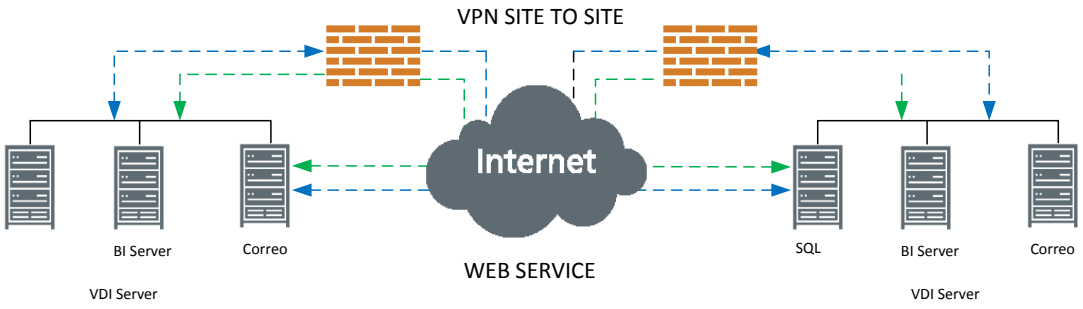


Grafico 22. Infraestructura de replicación propuesta para la EMPRESA REYES & HERMANOS.
. Fuente Propia

La sincronización web para la replicación de ambientes híbridos permite replicar datos utilizando el protocolo HTTPS y es útil en los siguientes escenarios:

- Sincronizar datos de usuarios móviles a través de Internet
- Sincronizar datos entre bases de datos de Microsoft SQL Server a través de un firewall corporativo

Su funcionamiento es el siguiente:

Agente de instalar un agente suscriptor. El agente realiza las tareas siguientes:

- Establece una conexión SQL con la base de datos de suscripciones.
- Extrae cualquier cambio de la base de datos.
- Realiza una solicitud HTTPS al equipo en el que se ejecuta IIS.
- Carga los cambios en los datos como un mensaje XML.

El Agente de replicación verifica la conexión del SQL Server hospedados en el equipo en el que se ejecuta IIS realizan lo siguiente:

- Responden a la solicitud HTTPS.
- Establecen una conexión SQL con la base de datos de publicación.
- Aplican los cambios de carga en la base de datos de publicación.
- Extraen los cambios de descarga para el suscriptor.
- Devuelven una respuesta HTTPS al Agente de mezcla.
- A continuación, el Agente se comunica con el suscriptor acepta la respuesta HTTPS y aplica los cambios de descarga a la base de datos de suscripciones.

6.3 Alta Disponibilidad

Se implementara un sistema de alta disponibilidad en servidores, nuevos servicio de comunicaciones y equipos de seguridad, esto le garantizara a la empresa tener servicios disponibles 99.98 % del tiempo. El objetivo concreto de

este sistema es proporcionar a los usuarios la disponibilidad permanente al momento de acceder a los servicios y recursos de TI.

El sistema de alta disponibilidad estará apoyado en la tecnología de virtualización de VMWARE lo que permitirá tener alta disponibilidad local y replicar una copia exacta de los servicios a la nube, otras de las bondades de esta tecnología es que tendrá la capacidad de administrar o balancear la carga de los servicios, garantizando esto una mayor velocidad en los sistemas y mejor tiempo de respuestas en los servicios navegación y correo electrónico.

Con este diseño los empleados de la empresa podrá conectarse desde cualquier punto en dado caso que existan una siniestro localmente, nuestro tiempo de recuperación ante el mismo dependería simplemente de un servicio de internet en la zona donde quisiéramos realizar la recuperación del mismo, en la figura siguiente se muestra esquema conceptual del el ambiente de alta disponibilidad de los servidores locales y la replicación en la nube.

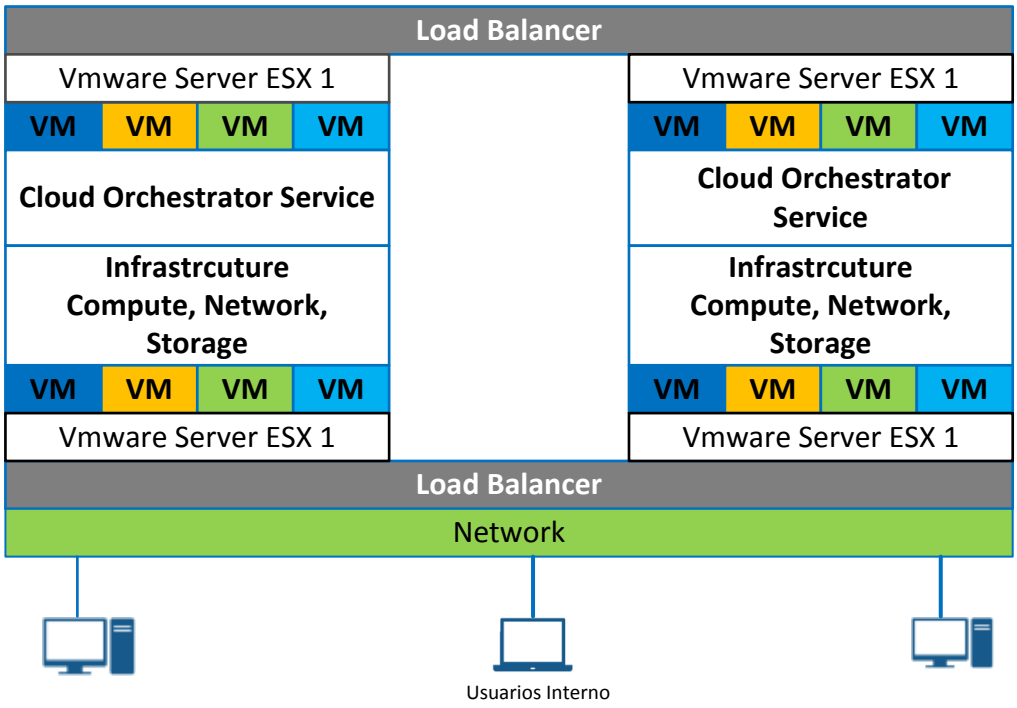


Grafico 23. Sistema de Alta Disponibilidad Propuesto Para la EMPRESA REYES Y HERMANOS. Fuente Propia

En un ambiente de alta disponibilidad existen varios factores los cuales hacen que un proyecto de esta magnitud sea exitoso, algunos de ellos son: equipos de comunicaciones, proveedores de servicio, diseño y una buena configuración estratégica, nuestro proyecto se apoya en tener equipos redundantes de comunicaciones y contrato de servicios con diferentes proveedores de telecomunicaciones.

Los empresa que son representantes de equipos y servicio juegan también un factor importante ya que nos da la garantía de soporte local y garantías de los equipos, Los equipos de comunicación que utilizaremos serán CISCO e

involucra la adquirió la re-utilización de , Switches , Routers, y balanceadores de carga, basándonos en una estructura distribuida inteligente utilizaremos configuraciones basadas en protocolo VRRP (Virtual Routers Redundancy Protocol) y protcolos con vector de distancia (RIP, IGRP) los mismos basados en algoritmos de estado de enlace mediante protocolos como OSPF, estos nos asegura que los datos inteligentemente utilicen el canal que esté disponible en ese momento.

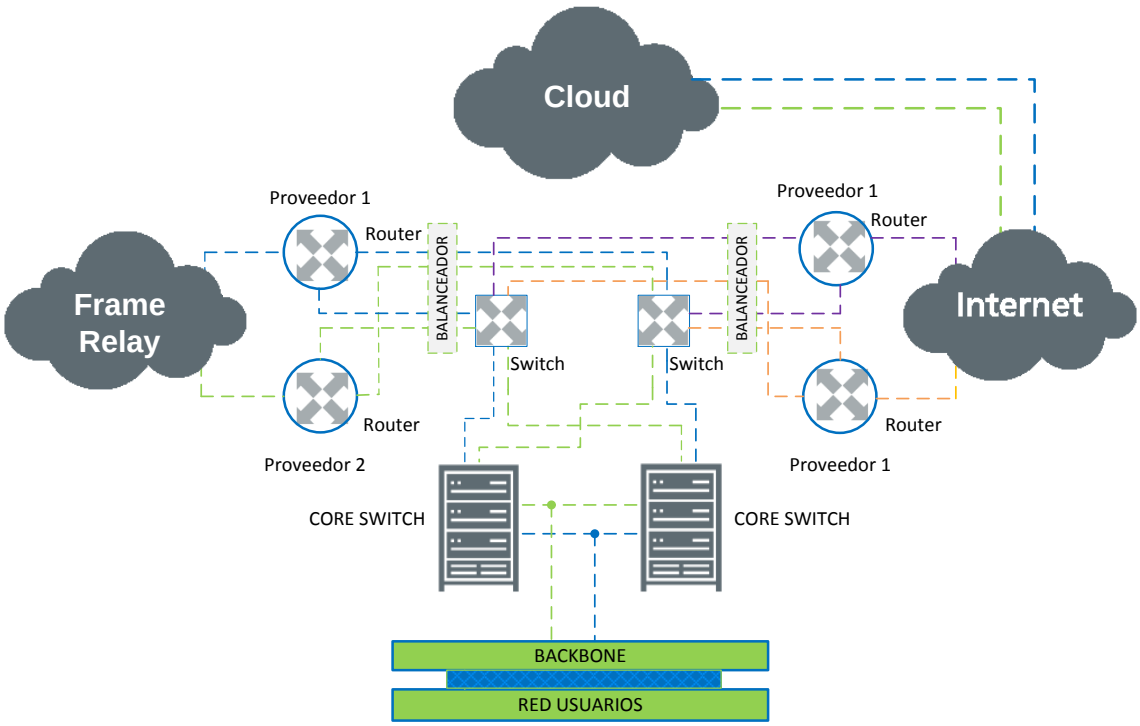


Grafico 24. Estructura de Comunicación propuesta para la EMPRESA REYES & HERMANOS. Fuente Propia

Tal y como se muestra en el grafico 24, la estructura de comunicación a implementar está enfocado en tener un ambiente hibrido (Activo-Activo, Activo-Pasivo, y Balanceo de carga) con esta estructura el administrador también podrá decidir si pasar a uno de estos tres estados de forma manual, en dado caso que necesite realizar un mantenimiento o simulacros de rutina.

6.4 Software Como Servicio

Se implementaran soluciones software como servicios para garantizar la disponibilidad de los servicios siguientes: Intranet, Extranet, Base de datos, correo electrónico, ventas móviles y productos de seguridad, dichas soluciones estarán bajo un ambiente de configuración hibrida de replicación otras en sincronización a través de servicios WEB (Web Service), tal como se muestra en el grafico 25.

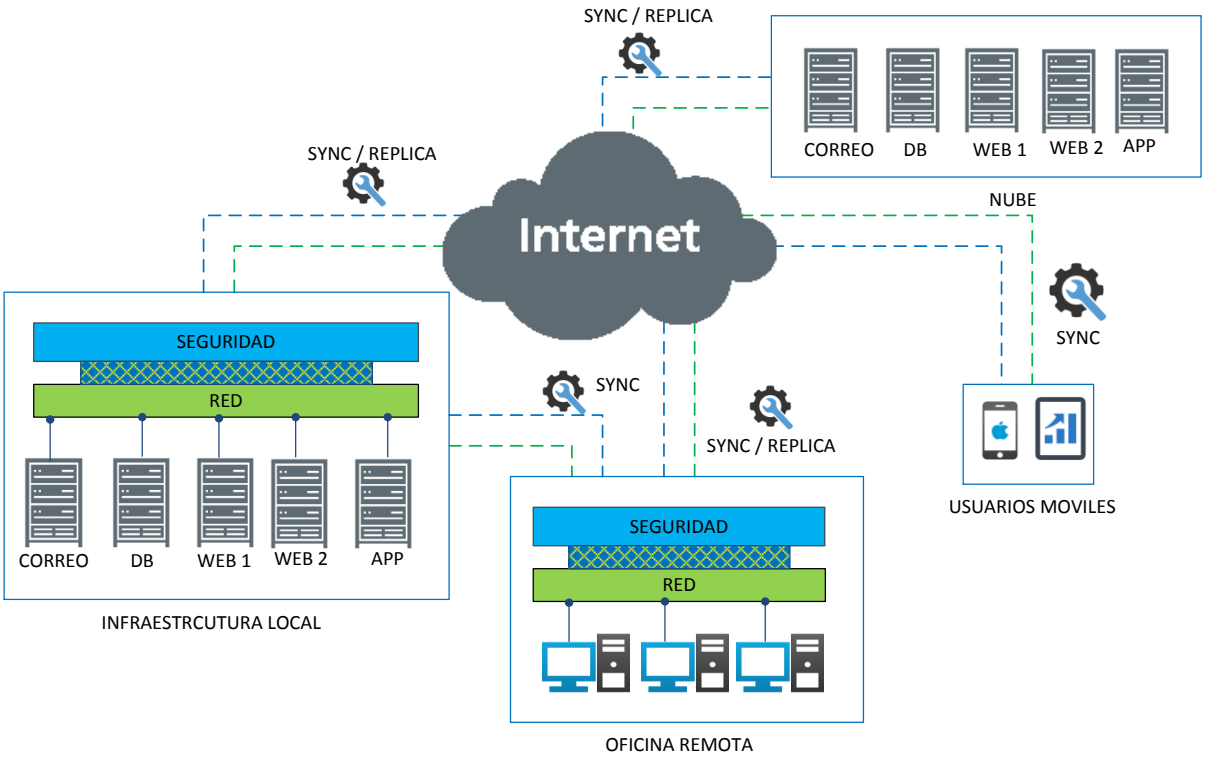


Grafico 25 Estructura de Software como servicio propuesta para la EMPRESA REYES & HERMANOS. Fuente Propia

Con la implementación de esta tecnología se trasmiten inmediatamente un ahorro, debido a que evita a la adquisición de activos y servicios para realizar un sitio alterno o un sitio de contingencia para el centro de datos

Ahorros

- Energía Eléctrica
- Sistema de enfriamiento
- Compra de equipos de informática como de comunicaciones
- Licenciamiento de software
- Personal de monitoreo y administración

- Certificación del data center
- Seguridad

Cuando la empresa adquiere este servicio a nivel financiero esto se traduce como un gasto, lo cual se transfiere en un ahorro para el negocio ya que al momento de presentar el pago de impuesto los mismos son descontados de dicho pago o acreditados.

Beneficios del Software como Servicio como parte de nuestro plan

Menos inversión inicial y menos riesgo: Al utilizar el software como servicio sin tener que realizar una inversión inicial en máquinas, ni en licenciamiento software base (SO) es un beneficio importante para los directores de IT y en definitiva para la empresa.

Reducción de Costes: Pagar por solo aquello que necesites, obtienes un ahorro de costes de mantenimiento de la plataforma de máquinas y del software necesario.

Actualizaciones y Nuevas Funcionalidades Inmediatas: No se requiere de personal dedicado para realizar los mantenimientos de las actualizaciones, dispondremos de las actualizaciones y mejoras del software de manera inmediata. En ocasiones podremos elegir el uso de nuevas funcionalidades.

Soporte más Ágil y Rápido: Los problemas de aplicación o fallas tienen un tratamiento directo ya que pueden afectar un radio mucho más grande de clientes, que las que son desarrolladas en casa.

6.5 Seguridad Como Servicio

Se implementara un sistema de protección de correo en la cual los mensajes Spam, Virus, Spayware, se direccionara a un tercero en este caso McAfee, esta empresa se encargara de entregarnos los correos limpios de todos tipos de amenazas, así como también tendremos la capacidad de configurar políticas para bloqueo y protección de pérdida de datos de la empresa a través del correo.

El fabricante McAfee como contingencia también ofrece un servicio hibrido, el cual nos proporciona un equipo instalado en nuestro Datacenter local, si falla su servicio tendremos la misma protección y si nuestro servicio falla por conectividad también seguiremos recibiendo correo en la plataforma de correo de Mcafee, cuando se restablezca los mensajes llegaran a nuestros servidores de correo. La implementación de ese servicio nos ahorrara, espacio en disco de nuestros servicios de correo ya que los mensajes de correo no deseados, virus no se mantendrán en nuestro servidor de correo, también el consumo de ancho de banda disminuirá, debido a que todo el tráfico malicioso y de correo basura se direccionara a McAfee. En la grafico 26 se muestra como el esquema de funcionamiento de este servicio.

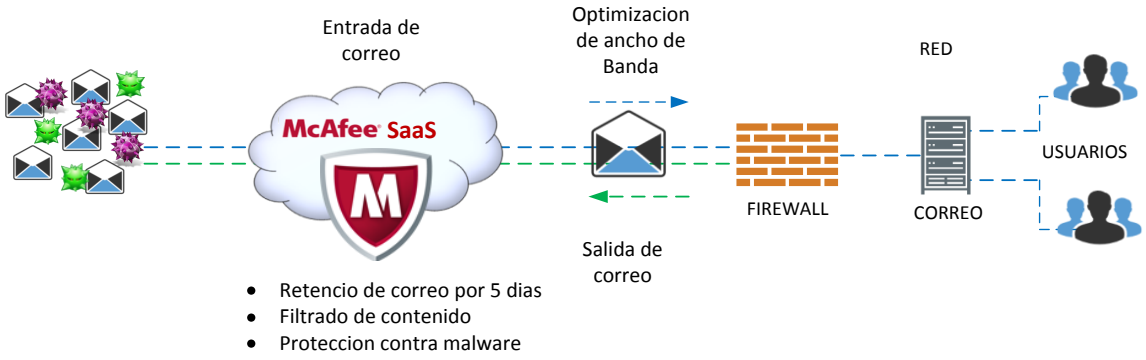


Grafico 26. Servicio de seguridad como servicio propuesto para la EMPRESA REYES & HERMANOS. Fuente Propia

Otras de las soluciones a implementar para garantizar los servicios de navegación, replicación de los datos a la nube, la seguridad de la información y la conexión con nuestros asociados a través de la red virtual privada (VPN) es un Firewall adicional al que tenemos actualmente, así como también la contratación de 3 proveedores de internet diferentes, para que en dado caso que alguno de ellos falle tener dos respaldos disponibles.

Estos servicios aunque estén como respaldo también se utilizaran para optimizar el servicio de navegación, debido a que la tecnología utilizada por el Firewall del fabricante sonicwall permite unificar estas tres líneas de internet y verlas como si fuese uno obteniendo así la suma de todos los anchos de banda de cada uno de los proveedores de internet y al mismo tiempo tener alta disponibilidad del equipo, líneas de internet y distribución de carga (Fail –Over, Load Balacing) esto nos proporciona una mejora en los servicios de un 95% así

como también nos provee diferentes capas de seguridad para la protección perimetral de nuestra empresa. Tal como se muestra en el grafico 27.

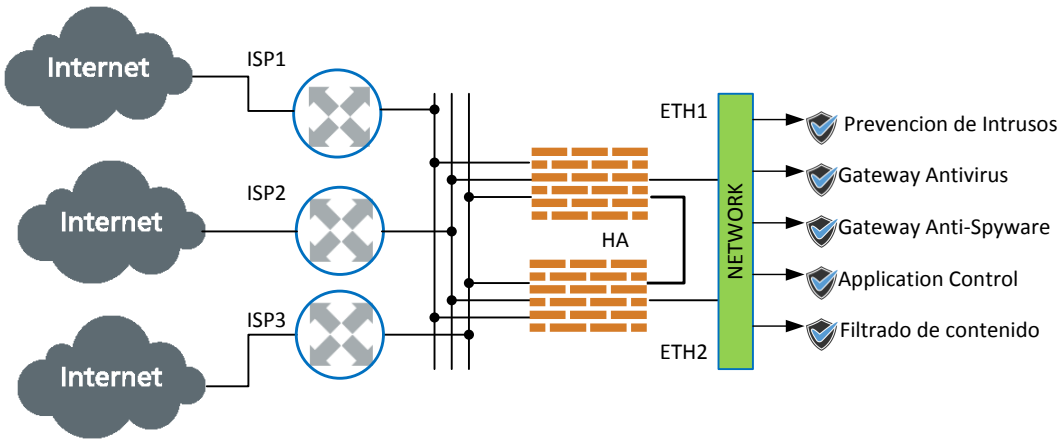


Grafico 27. Configuración de cluster de Firewall de seguridad propuesto para la EMPRESA REYES & HERMANOS. Fuente Propia

Con esta solución se resolverán algunas debilidades que tiene la infraestructura de Tecnología de la información (TI) de la empresa, las cuales provocaban que los servicios de navegación y la conectividad de la red virtual funcionaran muy lentas, ahora con la integración de los servicios de seguridad podremos integrarlo al directorio activo y configurar políticas por grupo de usuarios o usuarios en específico, y bloquear por categorías, controlar aplicaciones basadas en Web 2.0 y ancho de banda. Otras de las bondades de esta solución es que dentro de la suite de productos de seguridad es incluida la protección contra ataques día cero y prevención de intrusos esto nos garantiza que estaremos protegidos ante cualquier ataque de un hacker o de alguna amenaza

tanto externa como interna. Adicional esto tenemos la opción de seleccionar con cuales países quisiéramos tener conectividad a través de las opciones de geolocalización, con esta función filtraremos casi el 80% de las conexiones no deseadas que recibimos diariamente, lo que se transmite en ahorro de costos en análisis forense y administración de estos equipos. En el grafico 28 se muestra el diseño completo del sistema de continuidad de negocios basado en la nube (hibrido).

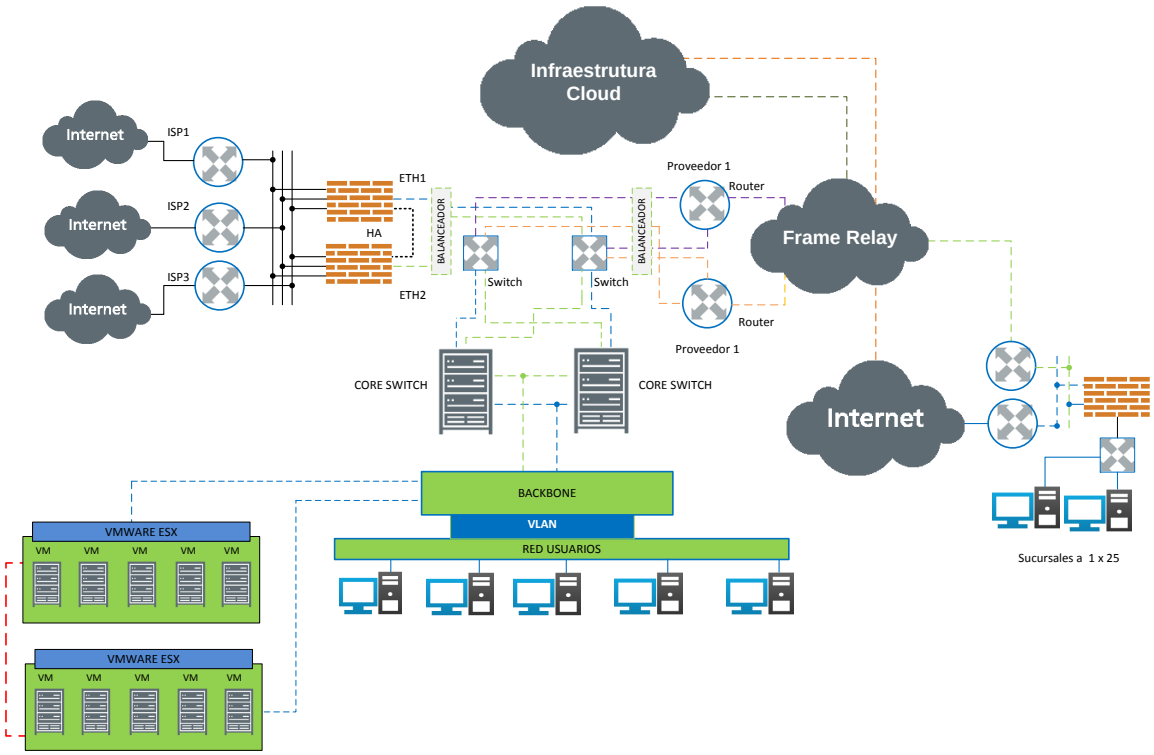


Grafico 28:Diseño de continuidad de negocio basado en la nube (hibidro) Propuesto para la EMPRESA REYES & HERMANOS. Fuente Propia

RESULTADOS

Con la implementación de esta sistema Continuidad de Negocio y Recuperación de Desastres Basada en la Nube, la empresa asegurara su activo más importante que es la información, además a tener un sistema de alta disponibilidad en su operaciones tecnológicas y recuperarse en un tiempo reducido, ante cualquier siniestro o eventualidad., basados en las encuestas realizadas indican que le empresa pierde alrededor de 10 millones de pesos mensuales fallas en los servicios de tecnología, en el grafico 29 se representan los más comunes. Con instalación de los equipos de alta disponibilidad y servicios redundantes de comunicaciones, los cuales forman parte de las herramientas de un plan de continuidad de negocios la empresa se estaría ahorrando 5 a 6 millones de pesos, más un aumento en la productividad de aproximadamente un 70% como lo indica la gráfica 29

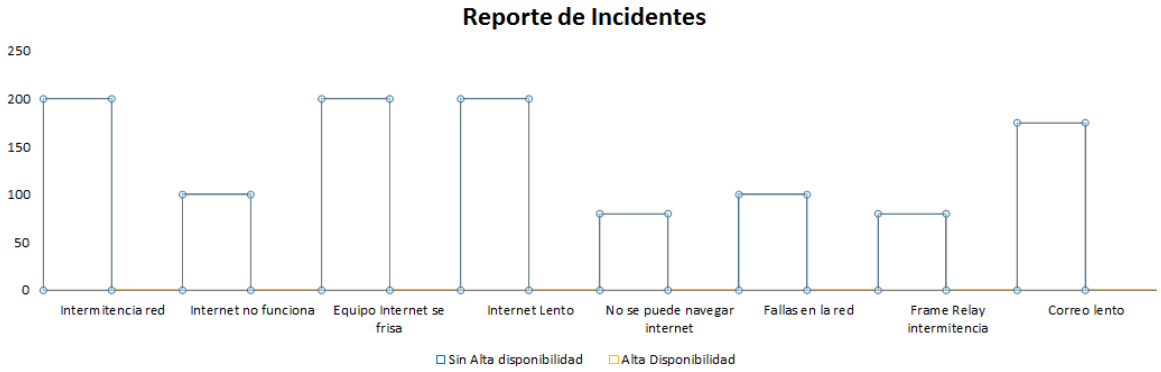


Grafico 29: Reporte comparativo con alta disponibilidad y sin alta disponibilidad de los equipos de comunicaciones sistemas de la EMPRESA REYES & HERMANOS.

Fuente Propia

A través de esta implantación la empresa tendrá la opción de hacer disponible las aplicaciones en dispositivos móviles, esto potenciara los ingresos por ventas, debido a que estas serán registradas en línea, en este sentido, la gerencia tendrá el poder de la información en tiempo real, teniendo opción de tomar decisiones basadas en información de tiempo real.

El cuerpo directivo podrá monitorear sus procesos vitales desde cualquier dispositivo en cualquier lugar donde haya disponibilidad de internet.

Con esta implementación la empresa obtendrá un diseño de alta disponibilidad de los servicios críticos, mayor productividad y ventajas competitivas, el cual puedan catapultara ofrecer servicios de calidad mundial y a explorar nuevas alianzas de negocios fuera de nuestro territorio.

La EMPRESA REYES & HERMANOS no tendrá una solución de continuidad de negocio propietario, lo que reduce los altos costos de mantenimientos de infraestructura tecnológica, regulaciones, cumplimiento de estándares y la inversión de un personal altamente calificado para la gestión técnica de la misma.

CONCLUSION

La EMPRESA REYES & HERMANOS tiene alrededor de 25 sucursales locales e internacionales, la misma se apoya en los sistemas de gestión de información para realizar sus procesos de producción, compra, ventas y distribución de sus productos. Al carecer de un sistema de continuidad de negocio para los sistemas de información, cada vez que ocurre una falla se ven afectadas todas las operaciones de la empresa, traduciéndose en pérdidas económicas, retrasos y deterioro de su imagen.

Para lograr sus objetivos de ser una empresa más competitiva, decidieron embarcarse en el proyecto de continuidad de negocios basado en un esquema hibrido de computación en la nube (Cloud Computing) e infraestructura local, el cual les permitirá tener sus operaciones 98.9% disponible, no solamente en el ámbito local sino también en el internacional.

Este sistema permite la integración de la infraestructura actual con la adquisición de servicio en la nube, asegurando que este proyecto sea costo-efectivo para la empresa. Esto proporcionara a la organización mayor velocidad y rentabilidad en sus procesos de negocio, aprovechando las nuevas tecnologías, podrán involucrarse en nuevos proyectos de movilidad para sus canales de distribución, asociados y a clientes finales.

Anteriormente, debido a las fallas del sistema, se realizaban procesos manuales y se duplicaba información, creando frustraciones en los usuarios porque tenían que realizar procesos repetitivitos, los cuales, retrasaban las tareas rutinarias entre 6 a 8 horas. Debido a esta situación, las operaciones vitales eran afectadas.

Con la implementación de la continuidad de negocios basada en la nube, todos estos procesos frustrantes serán erradicados, aumentando la productividad, disminuyendo costos y situando a la EMPRESA REYES & HERMANOS en una posición competitiva frente al mercado global.

BIBLIOGRAFIA

- Abad A.D. (2013). *Seguridad y alta disponibilidad. ISBN: 9788415452638, Ediciones Garceta,* **España.**
- Backups de bases de datos fuera del sitio: Almacenamiento en la nube*. (20 de mayo 2010). Obtenido de http://www.cioal.com/whitepapers/oracle/DB_LA_SP_WP_CloudStored.pdf*
- Fundación de la Innovación Bankinter (2010), *Cloud Computing La tercera ola de las tecnologías de la Información. Madrid,* **España.**
- Beltran M., Sevillano F. (2013). *Cloud Computing, tecnología y negocio. ISBN: 978-84-283-3514-0, Ediciones Paraninfo,* **España.**
- Bonet S., González F., Oltra R., Conchado A., Guzmán A. y Cebrián C. (2012). *Análisis de la oferta y la demanda de los servicios Cloud Computing. Editorial: AIMME - Instituto Tecnológico Metalmecánic, Valencia,* **España.**
- Borrow P. (2001), *Como preparar y poner en marcha planes de negocios, ISBN: 978-84-8088-800-4, Ediciones gestión 2000, Barcelona,* **España.**
- Carballar J. (2006), *Firewall: La seguridad de la banda ancha. ISBN: 978-84-7897-703-1, Ediciones Ra-Ma.* **España.**
- Contreras J. J. (2012), *Computación en la nube. Revista de divulgación científica Ciencia cierta.*

- Departamento de salud y Servicios Humanos de los EE.UU. Privacidad de información médica, extraído de http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html
- Díaz J. C. (2010), *Introducción al Business Intelligence, ISBN: 978-84-9788-886-8, Editorial UOC, Barcelona,* **España.**
- Furth B., Escalante A. (2012), Handbook of Cloud Computing, ISBN: 978-1441965233, Publisher: Springer, NY, **USA**.
- Gaspar J. (2004), *Planes de Contingencia la Continuidad Del Negocio en Las Organizaciones. ISBN: 84-7978-647-7, Ediciones Díaz de Santos, Madrid,* **España.**
- Gaspar J. (2006), *Planes de Contingencia la Continuidad Guía práctica para su elaboración. ISBN: 84-7978-778-3, Ediciones Díaz de Santos, Madrid,* **España.**
- Gómez Álvaro (2011a). *Seguridad Informática. Básico. ISBN: 9789586487214, Ecoe Ediciones,* **México**.
- Gómez Álvaro (2011b). *Auditoría Seguridad Informática. ISBN 9788492650743, STARBOOK EDITORIAL*, **México.**
- Gómez J. (2013). *Guía para implementar buenas prácticas globales en la Continuidad del Negocio. Edición global español,* **España.**
- Hoffer J. (enero 2001). *"Backing Up Business - Industry Trend or Event", Health Management Technology, recuperado*

de http://archive.is/20120629133345/findarticles.com/p/articles/mi_m0DUD/is_1_22/ai_68864006

- IDG Communication (2010), Libro blanco “Hablando Cloud”, el punto de referencia sobre el Cloud Computing y la nube privada. Microsoft.
- Industrias de tarjeta de pagos (PCI), Normas de seguridad de datos, *Requisitos y cumplimientos de evaluación de seguridad (octubre 2008) Zxtraído de* https://www.pcisecuritystandards.org/pdfs/pci_dss_spanish.pdf
- Instituto Nacional de Tecnologías de la Comunicación (2010), *El estudio sobre el estado de la PYME española ante los riesgos y la implantación de Planes de Continuidad de Negocio. Ediciones España de creative Commons,* **España.**
- Instituto Nacional de Tecnologías de la Comunicación (2012), *Estudio sobre seguridad de la información y continuidad de negocio en las pymes españolas. Ediciones España de creative Commons,* **España.**
- INTECO (Instituto Nacional de Tecnologías de la comunicación). (2011), Riesgos y amenazas en Cloud Computing. Obtenido de http://cert.inteco.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_riesgos_y_amenazas_en_cloud_computing.pdf
- ISO 22301: Impulsando el Desarrollo Tecnológico, extraído el 14 de enero de 2014 desde http://normaiso22301.com/continuidad-del-negocio-sistemas-cloud/.

- Joyanes L. (2012a), *Computación en la nube ESTRATEGIAS DE CLOUD COMPUTecnologia de la Informacion (TI)NG EN LAS EMPRESAS (1a edición). ISBN: 978-607-707-468-7, Ediciones Alfaomega*, **México**.
- Joyanes L. (2012b). Computación en la nube: Estado del arte. Ediciones Alfaomega, DF, **México.**
- Lener (Departamento de Propiedad Industrial, Intelectual y Tecnológica). 14 de abril de 2010, Aspectos Legales del cloud computing extraído de http://www.slideshare.net/enekoariz/aspectos-legales-cloud-computing
- Neil A. (2012), Iniciativa *"trae tu propio dispositivo". CISCO System, Inc. obtenido de http://www.CISCO.com/web/solutions/trends/byod_smart_solution/docs/BYOD_Whitepaper.pdf*
- ONTSI (Observatorio Nacional de las Telecomunicaciones y de la SI) perteneciente al Ministerio de Industria, Energía y Turismo del Gobierno de España (2012), *Cloud Computing: Retos y Oportunidades,* **España.**
- Reis D. (2013*), Seguridad para la nube y la virtualizacion For Dummies. ISBN: 978-1-118-85095-4, John Wilwy & Sons, Inc. NJ*, **USA.**
- Royer J. M. (2004), *SEGURIDAD EN LA INFORMÁTecnologia de la Informacion (TI)CA DE EMPRESA: RIESGOS, AMENAZAS, PREVENCIÓN Y SOLUCIONES. ISBN: 9782746023048, Ediciones Eni, Paris,***Francia.**
- Shinder D. (2010), *The Enterprise Cloud,* **USA.**

- Sean R., Wells C., Eaton P., Geels D., Zhao B., Weatherspoon H., Kubiatowicz J.(2001) *Distributed Data Store, University of California, Berkeley.***USA***.*
- Torres J., Reig G., Gómez I. y Pegenaute X. (2009), *Una visión del Cloud Computing desde un aula de la UPC. Ediciones lulu.com, Sevilla,* **España.**
- Torres J. (2011a), *Empresas en la nube - Ventajas y retos del Cloud Computing (2a edición). ISBN: 978-84-939082-2-2-5, Ediciones Libros de cabecera, Barcelona,***España.**
- Torres J. (2011b), *Del cloud computing al big data, Visión introductoria para jóvenes emprendedores (1a edición), Ediciones España de Creative Commons, Barcelona,***España.**
- U.S InterAmerican Community Affairs, *U.S. Congress Sarbanes-Oxley Act of 2002,*obtenido de http://www.interamericanusa.com/articulos/Leyes/Ley-Sar-Oxley.htm
- William J. (2002), *Disaster Recovery Planning: Preparing for the Unthinkable (3ra edición). ISBN: 0130462829, Publisher: Prentice Hall,* **USA.**

ANEXOS

- ✓ **Anteproyecto**
- ✓ **Plantilla de análisis de impacto del negocio**
- ✓ **Plantilla Matriz de Riego**
- ✓ **Costos de Implementación**
- ✓ **Diseño del diagrama de red del sistema de continuidad de negocio basado en la nube.**

Decanato de Ingeniería e Informática
Escuela de Informática

"Análisis para la Implementación de un Modelo de Continuidad de Negocio y Recuperación de Desastres Basada en la Nube para la EMPRESA REYES & HERMANOS", Santo Domingo R.D. 2014"

Sustentantes:

Francis Subervi	**1998-2222**
Eduardo Pérez	**2007-2391**
Julio Reyes	**2001-0227**

Asesor:
Ingeniero Santo Navarro

Anteproyecto de la Monografía para Optar por el Título de:
Ingeniero en Sistemas

Distrito Nacional, República Dominicana
2014

“Análisis para la implementación de un modelo de Continuidad de Negocios y Recuperación de Desastres Basada en la Nube para la “EMPRESA REYES & HERMANOS”, Santo Domingo R.D. 2014

INDICE

SELECCIÓN DEL TÍTULO Y DEFINICIÓN DEL TEMA

Análisis para la implementación de un modelo de Continuidad de Negocios y Recuperación de Desastres Basada en la Nube para la EMPRESA REYES & HERMANOS", Santo Domingo R.D. 2014.

1.1 DEFINICIÓN DEL TEMA

En este trabajo de grado desarrolla la implementación de un modelo de continuidad de negocios y recuperación de desastres basado en la nube. Esta estructura apoyará a la empresa a tener un sistema de alta disponibilidad en su operación tecnológica y recuperarse en un tiempo reducido, ante cualquier siniestro o eventualidad.

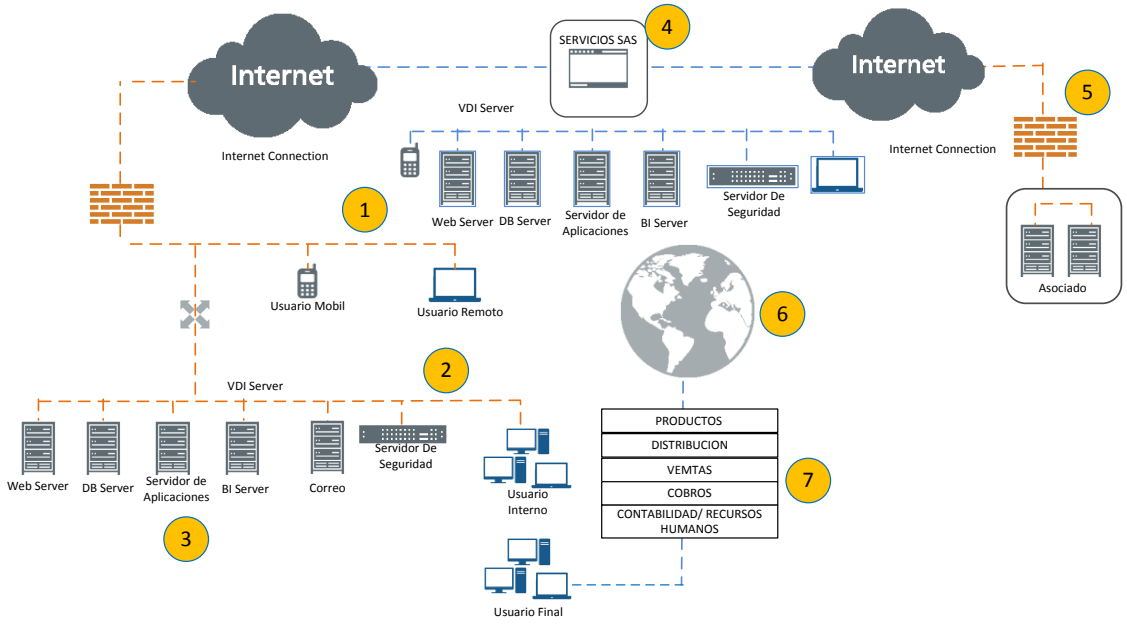


Gráfico 1; Fuente: Propia

1.2 ORGANIZACIÓN DE CONTENIDOS

Esta investigación estará dividida en capítulos, de la manera siguiente:

CAPITULO 1 - Se dará información organizacional de la EMPRESA REYES & HERMANOS.

CAPÍTULO 2 -Se dará una breve definición de todos los conceptos generales de la investigación.

CAPÍTULO3-Se definen los sistemas de continuidad de negocios basado en la nube.

CAPÍTULO4- Se desarrollan los aspectos importantes sobre la Infraestructura Tecnológicade la EMPRESA REYES & HERMANOS.

CAPÍTULO 5- Se dará una breve explicación sobre los sistemas actuales que usa la empresa.

CAPÍTULO6- Se definirá y se dará una breve explicación sobre la propuesta del sistema de continuidad de negocios y recuperación de desastres basado en la nube, además, las ventajas a nivel de seguridad de este sistema.

CAPÍTULO7 - Se realizará un estudio sobre los resultados y beneficios económicos de esta implementación.

CAPÍTULO 8- Se presentarán las conclusiones de la investigación.

CAPÍTULO 9- Se presenta la bibliografía consultada en el transcurso de la investigación.

2. PLANTEAMIENTO DEL PROBLEMA

En un estudio realizado por la empresa consultora globalcontinuity, se llegó a la conclusión de que las pérdidas financieras asociadas a las Interrupciones de servicio TI se disparan cuanto más tiempo tardan en resolverse.[1]

Según "TheAvoidableCost of Downtime" los departamentos más afectados por el tiempo de inactividad son las operaciones (62%), finanzas (48%) y adquisiciones (39%), para Estados Unidos.

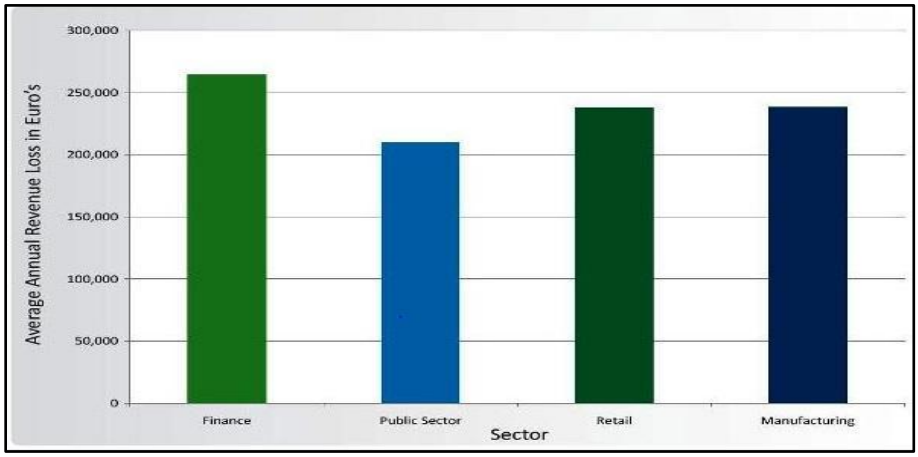


Grafico 1. El costo evitable de tempo de inactividad Fuente propia basada en el reporte de Computer Associate the impact of IT downtime on employee productivity

Para el caso de Europa el informe 'Avoidable Cost of Downtime 2010', realizado por la firma de investigación independiente Coleman Parkes a petición de CA Technologies, estima que las pérdidas financieras asociadas a las interrupciones

de servicio TI y al tiempo que tardan en recuperarlo, alcanzan los 3,000 millones.Los resultados de este estudio evidencian también que cada firma española registra una media de diez horas de interrupción del servicio TI al año, esto es más de 90.000 horas en el conjunto de España.

Y cuando los sistemas TI importantes no funcionan, las organizaciones estiman que su capacidad para generar ingresos queda reducida a un 36%. Los departamentos que más se ven afectados por estas interrupciones son los de Operaciones (62%), Ventas (52%) y Finanzas (52%).[2]

La EMPRESA REYES & HERMANOS no cuenta con un emplazamiento en la nube para planificación de continuidad del negocios (BC) y recuperación ante desastres (DR) que aborde incidentes como cortes de corriente, incendios, inundaciones, huracanes, terremotos, tornados e incluso robo, esto afecta la productividad del negocio e imagen de la empresa.

Tener una solución de continuidad de negocio propietario involucra altos costo de infraestructura tecnológica, regulaciones, cumplimiento de estándares y personal altamente calificado para la gestión técnica.Por otro lado, se suma la responsabilidad de la seguridad de la información y el almacenamiento de grandes volúmenes de información.

2 - Recuperado:http://www.computing.es/infraestructuras/tendencias/1034402001801/coste-interrupciones-servicio-espana.1.html:

OBJETIVOS DE LA INVESTIGACIÓN

3.1 OBJETIVO GENERAL

Optimización de la operación tecnológica para asegurar la continuidad de los procesos, logrando una reducción de costos por fallas, mediante un esquema de continuidad de negocios y recuperación de desastres basado en la nube.

3.2 OBJETIVOS ESPECÍFICOS

- Mejorar la operación tecnológica, bajo un enfoque de continuidad de negocios y recuperación de desastres basado en la nube.
- Crear un plan de contingencia operativa que permita la recuperación y continuidad de la empresa frente a fallas y/o desastres basada en un estándar de recuperación de desastres.
- Incrementar la capacidad de acceso a los servicios para apoyar la toma de decisiones.
- Disminución de costo ocasionado por fallas y/o desastres naturales o tecnológicos.
- Incrementar los niveles de satisfacción de clientes internos y externos, a través de la disponibilidad de los procesos.
- Identificar las necesidades de continuidad de servicios.

4. JUSTIFICACIÓN DE LA INVESTIGACIÓN

4.1 JUSTIFICACIÓN TEÓRICA

El Sistema de Gestión de la Continuidad del Negocio (SGCN) se ha convertido en una exigencia para las empresas que compiten el día de hoy en los mercados globalizados. La tendencia mundial es que ya las empresas no compitan entre sí: la competencia es entre cadenas de suministros. Una cadena de suministros, para mantenerse operando, no puede tener ningún eslabón débil; ninguno de sus componentes puede dejar de operar ya que si un elemento del todo dejara de funcionar se paraliza toda la serie, generando el caos.

Cada miembro del sistema tiene que demostrar que es un proveedor confiable. Esto se logra teniendo en cada empresa un SGCN que proteja a los procesos esenciales que permiten originar los productos o servicios que desea el cliente.[3]

Esta investigación busca mediante la aplicación de la teoría, observación y análisis, diseñar e implementar un modelo de continuidad de negocios y recuperación de desastres basado en la nube, que permita la disponibilidad de los procesos soportados por la operación tecnológica, tales como: Distribución, Ventas, Finanzas e Informes, con el objetivo de reducir costos por fallas y colocar la empresa en una posición de competitividad en el mercado.

3- Recuperado: http://www.gestion.com.do/index.php/octubre-2012/300-nuevo-estandar-internacional-en-continuidad-del-negocio-iso-223012012

4.2 JUSTIFICACIÓN METODOLÓGICA

Para cumplir con los objetivos del estudio de esta investigación se emplearán diversas técnicas que permitan identificar y analizar los factores que conlleva la implementación de la continuidad de negocios basada en la nube, esto involucra conocer los costos reales y ocultos de dichos servicios, los procesos de replicación de información, seguridad e integridad de los datos. Además de realizar análisis financiero lo cual involucra, personal de alto nivel, sistema de comunicación y tiempos de replicación y almacenamiento de datos.

4.3 JUSTIFICACIÓN PRÁCTICA

Con esta implementación se espera obtener un diseño de alta disponibilidad de los servicios críticos, mayor productividad y ventajas competitivas, el cual puedan catapultar a la empresa REYES COMPUTERS a ofrecer servicios de calidad mundial y a explorar nuevas alianzas de negocios fuera de nuestro territorio.´

5. TIPOS DE INVESTIGACIÓN

Para el desarrollo del trabajo de grado se utilizarán los siguientes tipos de investigación:

a) DESCRIPTIVA: Es un tipo de estudio que sirve para analizar cómo se manifiesta el objeto de investigación y sus componentes. Será utilizado en el desarrollo del trabajo para detallar los factores que involucra la implementación

de continuidad de negocios basado en la nube, también se utilizarán técnicas específicas en la recolección de información como son las entrevistas, observación y cuestionario, que ayudaran a identificar datos relevantes para la investigación.

b) EXPLICATIVA: Es un tipo estudio que busca encontrar las razones o causas que ocasionan ciertos fenómenos. Este será utilizado en todo el proceso para predefinir cada problema que pueda surgir, detallando los pasos para su resolución de forma clara y precisa, mediante un análisis, síntesis e interpretación de la información recolectada.

c) DOCUMENTAL: Es un tipo de estudio que busca indagar las causas en que generaron dicha necesidad. Este será utilizado en el trabajo de investigación, porque recolectamos una serie de información de la EMPRESA de REYES & HERMANOS el cual nos proporciona una serie de factores que justifican la implementación de continuidad de negocio basado en la nube.

d) ENTREVISTAS: Se utilizará esta técnica para la recolección o extracción de la información que será utilizada para el desarrollo del trabajo de investigación. Dichas entrevistas serán realizadas a todo el personal considerado clave o necesario, esto incluye directores, supervisores, técnicos involucrados y personal administrativo.

6. MARCOS DE REFERENCIA

6.1 MARCO TEÓRICO

La revolución tecnológica que actualmente estamos viviendo bien podría ser la más profunda de nuestra historia. Los servicios convergen y pasan del mundo físico al mundo digital, siendo accesibles desde cualquier dispositivo. Un hecho relevante es que nuestros datos ya no residen en nuestros ordenadores sino en una Internet Global que adquiere entidad propia y se convierte en mucho más que una simple infraestructura de conexión: es la plataforma que ofrece servicio a millones de dispositivos inteligentes conectados a la red (Torres, 2012).

La nube es la plataforma tecnológica por excelencia de la década actual y posiblemente, del futuro de la computación y se ha convertido en el término de moda de todos los medios de comunicación a nivel mundial (Joyanes, 2012).

La recuperación de desastres se está convirtiendo en un aspecto cada vez más importante de la informática empresarial. Como los dispositivos, sistemas y redes se vuelven cada vez más complejos, simplemente hay más cosas que pueden salir mal. Como consecuencia de ello, los planes de recuperación se han vuelto más complejos (William, 2002).

La seguridad de la información en sí es de importancia creciente, en parte porque la propia información puede ser vial, y hoy día se trata, transmite y almacena en sistemas de información soportados por tecnología, y también es

importante por los sucesos generales relacionados con la (in)seguridad en general: por todo ello las entidades han de contar con medios que puedan garantizar la continuidad de los sistemas y del negocio/servicio (Gaspar, 2004).

El ahorro de costes y la recuperación de desastres impulsan la adopción de sistemas CLOUD. Según las encuestas realizadas en sectores empresariales durante el año 2013, la adopción de sistemas de almacenamiento y aplicaciones Software en la nube es uno de los objetivos de la mayoría de las empresas a corto o medio plazo.

4- ISO 22301: Impulsando el Desarrollo Tecnológico, extraído el 14 de enero de 2014 desde http://normaiso22301.com/continuidad-del-negocio-sistemas-cloud/

La proliferación de dispositivos móviles en la fuerza de trabajo es un beneficio para las estrategias de continuidad del negocio, ya que le da más flexibilidad a las opciones de recuperación de la fuerza de trabajo. Los proveedores de software de planeamiento de la continuidad del negocio están poniendo más énfasis en asegurar que el software y la información que se requieren para la continuidad del negocio, pueda ser accesible mediante dispositivos móviles. Esto incluye información como el estado actual de la recuperación, las locaciones hacia las cuales deben ir los empleados, a qué aplicaciones y servicios pueden acceder, y dónde se conectan para conseguir las más recientes actualizaciones de emergencia. [5]

6.2 MARCO CONCEPTUAL

Recuperación de desastres:

Planificación e implementación de procedimientos e instalaciones para su uso cuando los sistemas esenciales no están disponibles por un periodo largo de tiempo lo suficientemente como para mantener un impacto significativo en el negocio. (The Free On-line Dictionary of Computing, © Denis Howe 2010).

Cloud Computing:

Computación en la nube es un modelo para permitir el acceso adecuado y bajo demanda a un conjunto de recursos de cómputo configurables (p.e. redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser rápidamente provistos y puestos a disposición del cliente con un mínimo esfuerzo de gestión y de interacción con el proveedor del servicio. Joyanes L. (2012).

SaaS (Software as a Service):

El software como servicio es un modelo de software basado en la Web que provee el software totalmente disponible a través de un navegador web. Las aplicaciones son accesibles desde diferentes dispositivos cliente a través de una interfaz cliente ligera tal como el citado navegador (p.e correo electrónico basado en web). Joyanes L. (2012).

Paas (Platform as a Service):

En el modelo de plataforma como servicio, el proveedor ofrece un entorno de desarrollo a los desarrolladores de aplicaciones, quienes desarrollan aplicaciones y ofrecen sus servicios a través de la plataforma del proveedor. El proveedor normalmente ofrece para el desarrollo " kits de herramientas lenguajes de programación, herramientas y estándares de desarrollo y canales de distribución y pago" y recibe un pago por proporcionar la plataforma y los servicios de distribución de ventas. Joyanes L. (2012).

5- Recuperado desde: http://cxo-community.com/articulos/blogs/blogs-seguridad-corporativa/4807-continuidad-del-negocio-ti-cuatro-tendencias-criticas.html

IaaS (Infrastructure as a Service):

El modelo IaaS proporciona la infraestructura necesaria para ejecutar aplicaciones. Este modelo ofrece espacio de almacenamiento, capacidad de proceso, servidores y otro equipamiento físico, en pago por uso. Puede incluir también, la entrega de sistemas operativos, redes y tecnología de vitalización para gestionar los recursos. Joyanes L. (2012).

Almacenamiento en la nube:

Un servicio que permite a los clientes ahorrar los datos mediante la transferencia a través de internet u otra red a un sistema de almacenamiento externo mantenido por un tercero. Shinder D. (2010).

Nubes públicas:

Se refieren al modelo estándar de computación en la nube, donde los servicios que se ofrecen se encuentran en servidores externos al usuario, pudiendo tener acceso a las aplicaciones de forma gratuita o de pago. Contreras J. J. (2012).

Nubes privadas:

En este grupo la plataforma se encuentra dentro de las instalaciones de la empresa y no suelen ofrecer servicios a terceros, en general, una nube privada es una plataforma para la obtención de hardware solamente, es decir, máquinas, almacenamiento e infraestructura de red (IaaS). Este tipo de nube privada es una buena opción para las compañías que necesitan alta protección de datos. El cliente controla qué aplicaciones usa y cómo, es el propietario de la infraestructura y puede decidir qué usuarios están autorizados a utilizarla. Contreras J. J. (2012).

Nubes hibridas:

Combinan recursos locales de una nube privada con la nube pública. La infraestructura privada se va aumentando con los servicios de computación en nube de la infraestructura pública, lo que permite a la empresa mantener el control de sus principales aplicaciones y datos y aprovechar la computación en nube pública solo cuando resulte necesario. Contreras J. J. (2012).

G-cloud (Government cloud o nube governmental):

Una nube gubernamental consiste en una nube privada en la que todos los servicios y recursos están dedicados a una Administración o Gobierno. La nube gubernamental puede ser interna, si las infraestructuras pertenecen al propio Gobierno, o externa, si las infraestructuras pertenecen a un proveedor. Fundación de la Innovación Bankinter (2010).

Virtualización:

La virtualización es un método de dividir un servidor físico en múltiples servidores ficticios o «virtuales», dando a cada uno el aspecto y la capacidad de estar funcionando en su propia máquina dedicada. Cada servidor virtual funciona como un servidor de pleno derecho y puede ser reiniciado de forma independiente. Este método permite equilibrar los recursos físicos entre los servidores virtuales en función de la demanda de cada uno. Fundación de la Innovación Bankinter (2010).

Data center:

Un centro de datos es una instalación utilizada para albergar sistemas de ordenadores y sus componentes asociados. Esta instalación concentra todos o parte de los recursos necesarios para el procesamiento de la información de una organización. Por lo general, incluyen fuentes de alimentación y conexiones de datos redundantes, copias de seguridad, sistemas de refrigeración y dispositivos de seguridad. Fundación de la Innovación Bankinter (2010).

Servidor virtual:

Un servidor virtual es una reproducción plenamente operativa de un servidor físico pero que no dispone de recursos computacionales dedicados, sino que los comparte con otros servidores virtuales por medio de la tecnología conocida como virtualización. Fundación de la Innovación Bankinter (2010).

Business continuity management:

Es un proceso de dirección que identifica los impactos potenciales que amenazan a la organización y proporciona el marco adecuado para construir y reforzar la capacidad de dar una respuesta efectiva que salvaguarde los intereses, la imagen y el valor de las actividades realizadas por la misma. Gaspar J. (2004).

Prevención de riesgos:

Son las medidas que se deberían tomar previamente para eliminar la posibilidad de que un riesgo se materialice. Gaspar J. (2004).

Reducción de riesgos:

Son las medidas a tomar previamente para reducir las posibilidades de que un riesgo se materialice. Gaspar J. (2004).

Operaciones de recuperación:

Son los procedimientos que deben estar desarrollados con anterioridad para definir las acciones que cada equipo de recuperación debe desempeñar a

continuación de las operaciones de respuestas para restaurar el nivel mínimo de actividad que se haya definido previamente. Gaspar J. (2004).

Gestión de crisis:

Son los procedimientos que deben estar desarrollados con anterioridad para manejar las comunicaciones al exterior durante la crisis. No solamente para informar a los medios de comunicación, sino también de cara a los empleados. Gaspar J. (2004).

6.3 MARCO ESPACIAL

La investigación será realizada en base a datos e informaciones obtenidas de la EMPRESA REYES & HERMANOS, Zona Industrial de Herrera, D.N. Santo Domingo.

6.4 MARCO TEMPORAL

La investigación será realizada en el periodo Enero – Abril 2014.

7. MÉTODOS, PROCEDIMIENTOS Y TÉCNICAS UTILIZADAS EN LA INVESTIGACIÓN

7.1 MÉTODO

Las metodologías que se utilizarán para este trabajo de grado son:

a) Método Observación: Se utilizará este método para realizar observaciones de la problemática planteada y el impacto que logrará la implementación de los

procesos virtuales en el modelo de continuidad de negocio basada en la nube en la empresa REYES & HERMANOS.

B) Método Inductivo: Se realizará un análisis ordenado, coherente y lógico de las situaciones observadas, el cual tendrá como objetivo confirmar los datos y hechos anteriormente observados.

c) Método Deductivo: Se utilizará este método el cuál será basado en la observación anteriormente realizada con la finalidad de señalar las particularidades del problema planteado.

d) Método de Análisis y Síntesis: Se utilizará este método debido a que se establecerán las razones de causa y efecto de los factores que provocan la problemática y, se realizará una síntesis del análisis realizado.

7.2 PROCEDIMIENTO

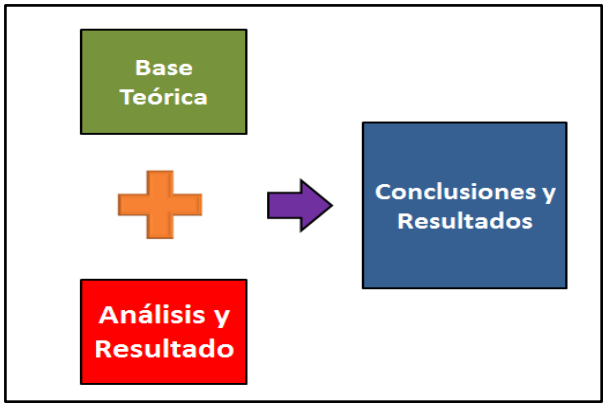
Luego de obtener las informaciones recolectadas mediante los métodos antes mencionados se realizarán las siguientes actividades:

- Definición conceptos generales, una base teórica para exponer los fundamentos y características de los temas. Esa base estará apoyada en libros técnicos y sitios web debidamente identificados.
- Análisis de la Infraestructura del sistema para la EMPRESA REYES & HERMANOS.

- Análisis del sistema o procesos contingencia actual de la para la EMPRESA REYES & HERMANOS.
- Desarrollar un modelo de Continuidad de Negocio y Recuperación de Desastres Basada en la Nube para la EMPRESA REYES & HERMANOS.

Finalmente se presentará un informe final del proyecto con las conclusiones y los resultados.

El esquema de la investigación será (ver gráfico 3):



7.3 TÉCNICA

Las técnicas utilizadas para la recolección de información de este trabajo de grado serán:

La entrevista: Se utilizará esta técnica para la recolección o extracción de la información que será utilizada para el desarrollo del trabajo de investigación. Dichas entrevistas serán realizadas a todo el personal considerado clave o

necesario, esto incluye directores, supervisores, técnicos involucrados y personal administrativo.

Caso de estudios: son herramientas que consisten en ejemplos reales en los que se presenta una historia positiva sobre los beneficios que un producto o servicio le han significado a determinados usuarios.

Artículos periodísticos: Es un texto que expresa la opinión que redacta el mismo público al cual es dirigido, con la finalidad de encontrar en el lector la formación de la opinión y el conocimiento del tema.

Documentos de investigación: Dan a conocer de un modo claro y preciso en lo posible, determinados conocimientos.

Informes técnicos: Método de análisis o para reportar aspectos técnicos del tema o problema específico y generar posibles soluciones.

TABLA DE CONTENIDO

Capitulo 1. Información organizacional

1.1. ¿Quiénes somos?

1.2. Misión

1.3. Visión

1.4. Objetivos

1.5. Valores

1.6. Estructura organizacional

Capitulo 2. Conceptos Generales

2.1. Computación en la nube

2.2. Interoperabilidad datos y Aplicaciones

2.3. Portabilidad

2.4. Gobernabilidad y gestión

2.5. Medición y Monitoreo

2.6. SLA

2.7. Virtualización de aplicaciones

2.8. Continuidad de negocios Tecnología de la Información (Siglas en Ingles IT)

2.9. Plan de recuperación de desastres (Disaster Recovery Plan, DRP)

2.10. Plan de continuidad de negocios (Business Continuity Planing, BCP)

2.11. Análisis de impacto del negocio (Business Impact Analysis, BIA)

2.12. Seguridad.

2.13. Riesgo y Cumplimiento

Capitulo 3. Sistema de continuidad de negocio

3.1. Sistema de continuidad basado en servicio

3.2. Sistema de continuidad basado en aplicaciones

3.3. Sistema de continuidad basado en la recuperación de desastres

3.4. Sistema de continuidad de respaldo basado en la nube

3.5. Sistema de continuidad de respaldo basado en almacenaje

3.6. Sistema de continuidad en servicios de seguridad

Capitulo 4. Infraestructura Tecnológica de la empresa

4.1. Centro de datos

4.2. Infraestructura virtual

4.3. Infraestructura de servidores

4.4. Infraestructura de comunicaciones

4.5. Infraestructura de red internacional

4.6. Estructura energética

Capitulo 5. Sistema de Información de la empresa

5.1. Sistema Financiero

5.2. Sistema de producción

5.3. Sistema de control de almacén

5.4. Sistema de Recursos Humanos

5.5. Sistema de respaldo local

Capitulo 6. Sistema de continuidad basado en la nube

6.1. Sistema de continuidad de negocio hibrido

6.2. Replicación

6.3. Alta disponibilidad

6.4. Software como servicio

6.5. Seguridad como servicio

RESULTADOS

CONCLUSION

BIBLIOGRAFIA

ANEXOS

BIBLIOGRAFIA

1. Abad A.D. (2013). Seguridad y alta disponibilidad. ISBN: 9788415452638, Ediciones Garceta, **España.**
2. Bonet S., González F., Oltra R., Conchado A., Guzmán A. y Cebrián C. (2012). Análisis de la oferta y la demanda de los servicios Cloud Computing. Editorial: AIMME - Instituto Tecnológico Metalmecánic, Valencia, **España.**
3. Borrow P. (2001), Como preparar y poner en marcha planes de negocios, ISBN: 978-84-8088-800-4, Ediciones gestión 2000, Barcelona, **España.**
4. Carballar J. (2006), Firewall: La seguridad de la banda ancha. ISBN: 978-84-7897-703-1, Ediciones Ra-Ma. **España.**
5. Contreras J. J. (2012), Computación en la nube. Revista de divulgación científica Ciencia cierta.
6. Díaz J. C. (2010), Introducción al Business Intelligence, ISBN: 978-84-9788-886-8, Editorial UOC, Barcelona, **España.**
7. Fundación de la Innovación Bankinter (2010), Cloud Computing La tercera ola de las tecnologías de la Información. Madrid, **España**.
8. Furth B., Escalante A. (2012), Handbook of Cloud Computing, ISBN: 978-1441965233, Publisher: Springer, NY, **USA**.
9. Gaspar J. (2004), Planes de Contingencia la Continuidad Del Negocio en Las Organizaciones. ISBN: 84-7978-647-7, Ediciones Díaz de Santos, Madrid, **España.**

10. Gaspar J. (2006), Planes de Contingencia la Continuidad Guía práctica para su elaboración. ISBN: 84-7978-778-3, Ediciones Díaz de Santos, Madrid, **España.**

11. Gómez Álvaro (2011a). Seguridad Informática. Básico. ISBN: 9789586487214, Ecoe Ediciones, **México**.

12. Gómez Álvaro (2011b). Auditoría Seguridad Informática. ISBN 9788492650743, STARBOOK EDITORIAL, **México.**

13. IDG Communication (2010), Libro blanco “Hablando Cloud”, el punto de referencia sobre el Cloud Computing y la nube privada. Microsoft.

14. Instituto Nacional de Tecnologías de la Comunicación (2010), El estudio sobre el estado de la PYME española ante los riesgos y la implantación de Planes de Continuidad de Negocio. Ediciones España de creative Commons, **España.**

15. Instituto Nacional de Tecnologías de la Comunicación (2012), Estudio sobre seguridad de la información y continuidad de negocio en las pymes españolas. Ediciones España de creative Commons, **España.**

16. ISO 22301: Impulsando el Desarrollo Tecnológico, extraído el 14 de enero de 2014 desde http://normaiso22301.com/continuidad-del-negocio-sistemas-cloud/.

17. Joyanes L. (2012a), Computación en la nube ESTRATEGIAS DE CLOUD COMPUTING EN LAS EMPRESAS (1a edición). ISBN: 978-607-707-468-7, Ediciones Alfaomega, **México**.

18. Joyanes L. (2012b). Computación en la nube: Estado del arte. Ediciones Alfaomega, DF, **México.**

19. ONTSI (Observatorio Nacional de las Telecomunicaciones y de la SI) perteneciente al Ministerio de Industria, Energía y Turismo del Gobierno de España (2012), Cloud Computing: Retos y Oportunidades, **España.**

20. Royer J. M. (2004), SEGURIDAD EN LA INFORMÁTICA DE EMPRESA: RIESGOS, AMENAZAS, PREVENCIÓN Y SOLUCIONES. ISBN: 9782746023048, Ediciones Eni, Paris, **Francia.**

21. Shinder D. (2010), The Enterprise Cloud, **USA.**

22. Torres J., Reig G., Gómez I. y Pegenaute X. (2009), Una visión del Cloud Computing desde un aula de la UPC. Ediciones lulu.com, Sevilla, **España.**

23. Torres J. (2011a), Empresas en la nube - Ventajas y retos del Cloud Computing (2a edición). ISBN: 978-84-939082-2-2-5, Ediciones Libros de cabecera, Barcelona, **España.**

24. Torres J. (2011b), Del cloud computing al big data, Visión introductoria para jóvenes emprendedores (1a edición), Ediciones España de Creative Commons, Barcelona, **España.**

25. William J. (2002), Disaster Recovery Planning: Preparing for the Unthinkable (3ra edición). ISBN:0130462829, Publisher: Prentice Hall, **USA.**

REYES & HERMANOS
Análisis de Impacto al Negocio (BIA)

Presentado Por:		**Fecha Realización**	
Título:		**Fecha Entrevista:**	
Teléfono/Correo:		**Fecha Finalizado:**	
Aprobado Por:		**Fecha Firmado:**	

Unidad Empresarial/Perfil Departamento

1) Unidad Empresarial / Nombre Depart.:	Ubicación	Ciudad, Estado, ZIP

2) Procesos Críticos Números de Referencia		Tiempo Objetivo de Recuperación
1	Produccion	Priority 1: <24hrs
2	Distribucion	Priority 1: <24hrs
3	Ventas	Priority 1: <24hrs
4	Cobros	Priority 2: 25-48hrs
5	Contabilidad	Priority 2: 25-48hrs
6	Reporte	Priority 3: 49-72hrs

3) Impactos Monetarios:

El "Impacto Monetario" de un fallo debe ser considerado en términos tanto de la pérdida de ingresos como de los gastos incurridos. Cada proceso en los períodos de tiempo dados contiene un cuadro desplegable desde el cual un rango de impacto en pesos debe ser seleccionado. Los rangos en pesos son acumulativos, no graduales. Seleccionar un impacto en cada período de tiempo.

IMPACTO ACUMULATIVO EN EL TIEMPO (A la conclusión de cada período)							
Procesos Crítico (use número de referencia)	Ingresos/ Gastos	≤24hrs	≤48hrs	≤72hrs	≤7Días	≤14Días	≥14Días
1	Perdidas Financieras	< $1,000,000	< $2,000,000	< $2,000,000	< $2,000,000	< $2,000,000	>$5,000,000
2	Perdidas Financieras	< $500,000	< $500,000	< $1,000,000	< $1,000,000	< $2,000,000	< $5,000,000
3	Perdidas Financieras	< $250,000	< $500,000	< $500,000	< $1,000,000	< $1,000,000	>$5,000,000
4	Perdidas Financieras	< $250,000	< $500,000	< $500,000	< $1,000,000	< $2,000,000	>$5,000,000
5	Incurrencia a Gastos	<$50,000	<$50,000	<$100,000	<$100,000	<$100,000	< $250,000
6	Incurrencia a Gastos	<$50,000	<$50,000	<$50,000	<$50,000	<$50,000	<$100,000

4) Impactos No Monetarios:

Proporcione los "Impactos No Monetarios" de indisponibilidad de sus procesos críticos. No es necesario enumerar un proceso crítico si su interrupción no presentaría ningún impacto monetario. Si no hay ningun impacto en la primera columna, donde inicia los "indices", seleccione "None" hasta que llegue un momento en el que haya un impacto. Una vez que se alcanza el impacto mas alto, continúe seleccionando la respuesta hasta que haya completado la evaluación para cada período de tiempo.

Proceso Crítico (use número de referencia)	Tipo de Impacto	≤24hrs	≤48hrs	≤72hrs	≤7Días	≤14Días	≥14Días
1	Impacto Inversionista	1	1	2	2	3	3
2	Imagen/ Prestigio	None	None	1	1	2	3
3	Mercado	None	None	1	2	2	3
4	Impacto Inversionista	None	1	1	3	3	3
5	Impacto Inversionista	None	Ninguno	1	1	1	2
6	Impacto Inversionista	None	None	1	1	2	2

Índice de Calificaciones
1= Menor
2=Media
3=Severa
4=Catastrófica

5) Tecnología Crítica:

Aplicaciones	Procesos Críticos Soportados (Use los Números de Referencias de los Procesos Críticos del Párrafo 2)	RTO	RPO
ERP	1	Priority 1: <24hrs	None
ERP	2	Priority 1: <24hrs	None
ERP	3	Priority 1: <24hrs	None
ERP	4	Priority 2: 25-48hrs	None
ERP	5	Priority 2: 25-48hrs	None
ERP	6	Priority 3: 49-72hrs	<12 Hours

Ir al Detalle de Aplicaciones

Si los datos de este departamento se almacenan en la red, por favor identifique el nombre del recurso compartido (el formato es \ \ server \ compartir). (ejemplo: Disco H o Disco Departamental). Con ello se garantizará la identificación de otras bases de datos relacionadas con sus aplicaciones. Para RPO, proporcionar la cantidad de datos de estas bases de datos se pueden perder sin impacto catastrófico en sus procesos críticos y ABC	DISPONIBILIDAD DE ALMACEN DE DATOS	RTO	RPO

Servidores Propios de Unidad de Negocios	Si su departamento es responsible de un servidor o equipo que se encuentra en su área de trabajo, haga clic en el enlace a la derecha y proporcione la información solicitada.	Ir al Detalle de Servidores

6) Registros Vitales - Papel:

Registro Vital	Propósito / Descripción de Uso	RTO	Estos Registros se pueden obtener en otra parte?	Almacenados fuera del Sitio por ABC?
N/A				

7) Externo (Vendedores, Suplidores, etc.) Dependencias:

Nombre del Proveedor de Servicio Externo	Relación Contractual?	Nos Apoyamos en Ellos Para:	Han Estado Calificados?
CISCO			
HP			
Mcafee			
Adexsus			
Microsoft			

8) EQUIPO ESPECIALIZADO

Equipo Especializado	Procesos Críticos	RTO	Vendedor / Suplidor

Requisitos de reubicación Telecom
##

Ir al Detalle Telecom

9) REQUISITOS DE REUBICACIÓN DE ESTACIÓN DE TRABAJO DEL TRABAJADOR - Nota, una estación de trabajo se define como: un escritorio, silla, compañía estándar de imagen computarizada para su departamento / unidad de negocio, teléfono y acceso a: bases de datos, impresora, copiadora, fax.

THE NUMBERS UNDER EACH TIME FRAME ARE INCREMENTAL...NOT CUMULATIVE.

EQUIPO/GRUPO	PROCESO	PRIORIDAD 1 ≤24 Hrs	PRIORIDAD 2 ≤48Hrs	PRIORIDAD 3 <72 Hrs	PRIORIDAD 4 ≤7 Días	PRIORIDAD 5 ≤14 Días	PRIORIDAD 6 ≥14 Días	TOTAL
								0
								0
								0
								0
								0
								0
		0	0	0	0	0	0	0

REYES & HERMANOS

Matriz Evaluación de Riesgo Detallado - 2014

Nivel de Probabilidad: 1 - Raro / 5 - Casi Seguro	Nivel de Impacto: 1 - Insignificante / 5 - Catastrófico

0	1	2	3	4	5	6 Riesgo Absoluto			7
R #	**Activo / Procesos / Subproceso**	**Amenazas**	**Vulnerabilidad**	**Tipo de Riesgo**	**Dueño / Responsable**	**Impacto (1-5)**	**Probabilidad (1-5)**	**Clasif. Riesgo**	**Clave (Y/N)**
1	**Administracion infraestructura de TI**	Falta de recursos Tecnologicos para soportar las operaciones del negocio. Inadecuada administracion de los sistemas. (Licenciamiento)	Que existan servidores que no cuenten con los debidos sistemas actualizados.	Operativo	Tecnologia y Soporte tecnico	5	2	10	
2			Inexistencia de politicas y procedimientos para la restauracion del sistema.	Operativo	Tecnologia y Soporte tecnico	4	3	12	
3			Que los sistemas instalados no esten cubiertos en su totalidad por la licencias existentes.	Cumplimiento	Gerenecia de tecnologia de la informacion	5	3	15	
4			Inadecuada administracion prosupuestaria para la adquisicion de los equipos tecnologicos.	Operativo	Director TI	3	3	9	
5								0	
6								0	
7								0	
8								0	
9								0	
10								0	
11	**Base de datos**	Base de datos sin actualizar. Configuracion de seguridad ineficiente. Malware.	No establecer programa de backup	Operativo	Tecnologia y Soporte tecnico	4	3	12	
12			Ataques malintencionados	Operativo	Seguridad de la informacion	4	3	12	
13			Privilegios otorgados que exceden los requerimientos del puesto de trabajo.	Operativo	gerenecia de tecnologia de la informacion	4	3	12	
14			Robos de discos y de cintas	Operativo	seguridad de la informacion y Seguridad fisica	5	3	15	
15								0	
16								0	
17								0	
18								0	
19								0	
20								0	
21								0	
22								0	
23								0	
24								0	
25								0	
26								0	
27	**Configuracion corta fuego (Firewalls)**	Penetracion a las redes, equipos y sistema de REYES & HERMANOS, por entes malicios que expongan los activos de la empresa	Inadecuada administracion de lo firewalls	Operativo	Seguridad de la informacion	4	2	8	
28			Falta de medidas proactivas para proteger la integridad de las redes y de la información.	Operativo	Seguridad de la informacion	4	2	8	
29			Usuarios con acceso a modificacion de configuracion de firewalls sin que pertenezcan al area correspondientes.	Operativo	Seguridad de la informacion	5	2	10	
30			Que no exista una herramienta automatizada para la prevencion de actividades maliciosas.	Operativo	Seguridad de la informacion	4	3	12	
31			Que las configuraciones de los firewalls no sean revisados periódicamente.	Operativo	Seguridad de la informacion	4	2	8	
32								0	
33								0	
34								0	
35								0	
36								0	
37								0	
38								0	
39								0	
40	**ERP**	Falta de conocimientos de los procesos actuales de la empresa REYES & HERMANOS. No generar una ventaja competitiva.	Indebida capacitacion al personal sobre los procesos	Operativo	Tecnologia y Soporte tecnico	4	2	8	
41			Falla de sistema	Operativo	Desarrollo	3	3	9	
42			Infeccion de virus	Operativo	Seguridad de la informacion	3	3	9	
43			Ataques de intrusos	Operativo	Seguridad de la informacion	5	3	15	
44			Informacion de mala calidad (No depurada)	Operativo	Desarrollo	2	2	4	
45			Falta de integridad en los datos	Operativo	Tecnologia y Soporte tecnico	4	2	8	
46								0	
47								0	
48								0	

R #	Activo / Procesos / Subproceso	Amenazas	Vulnerabilidad	Tipo de Riesgo	Dueño / Responsable	Impacto (1-5)	Probabilidad (1-5)	Clasif. Riesgo	Clave (Y/N)
49								0	
50								0	
51								0	
52								0	
53								0	
54								0	
55	Administracion Sala de Maquinas	Errores o fallas de los servicios, sistemas, equipos y las redes de la empresa REYES & Hermanos	Falta de conocimientos de todos los procesos claves.	Operativo	Seguridad de la informacion	4	3	12	
56			Que no existan sistemas de alertas, seguridad, controles de acceso.	Operativo	Seguridad de la informacion	4	2	8	
57			Existencia de empleados con acceso a sala de maquinas sin que su rol lo amerite.	Operativo	Seguridad de la informacion	3	3	9	
58			Incumplimientos de las politicas y los procedimientos.	Operativo	Gerenecia de tecnologia de la informacion	5	2	10	
59			Responsibilidades del departamento de TI no claras	Operativo	Gerenecia de tecnologia de la informacion	4	2	8	
60								0	
61								0	
62								0	
63								0	
64								0	
65	Recursos Humanos	Mal uso de los sistemas de informacion. Situaciones legales con empleados. Fraudes financieros u operativos.	Que el departamento de TI no programe adecuadas capacitaciones para su colaboradores.	Cumplimiento	RRHH y Gerencia de Tecnologia de Informacion	4	2	8	
66			Situaciones legales ante la falta de la no programacion de vacaciones.	Cumplimiento	RRHH	3	2	6	
67			Inexistencia de creaciones de descripcion de puestos.	Cumplimiento	RRHH	3	2	6	
68			Existencia de empleados con alto nivel de endeudamiento.	Cumplimiento	RRHH	2	3	6	
69								0	
70								0	
71								0	
72								0	
73								0	
74								0	
75								0	
76								0	
77								0	
78								0	
79	Eventos externos	Fenomenos naturales que pongan en riesgo la continuidad de REYES & HERMANOS. Situaciones con proveedores	No existencias de para-rayos, tierra electrica y extintores	Operativo	Seguridad Fisica	5	3	15	
80			No realizacion de revisiones/ mantenimiento continuo para la infraestructura fisica de REYES & HERMANOS.	Operativo	Seguridad Fisica	5	3	15	
81			No cumplimiento con las obligaciones legales.	Cumplimiento	Gerencia Administrativa.	4	2	8	
82			Pago inapropiado a los servicios de terceros.	Financiero	Gerenecia Administrativa.	4	2	8	
83			Inexistencia detectores de humo y falta de capacitacion al personal.	Cumplimiento	Seguridad Fisica	5	2	10	
84								0	
85								0	
86								0	
87								0	
88								0	
89								0	
90								0	
91								0	
92								0	
93								0	
94								0	
95								0	
96								0	

Presupuesto Implementacion Continuidad de Negocios Basado en la Nube (Hibidro)

# de Parte	Productos	Cantidad	Precio	Total
	Equipo Adicional para el Site Principal			
01-SSC-3863	**Sonicwall Firewall NSA 2600 Series TotalSecure** Comprehensive Gateway Security Suite includes - Gateway Anti-Virus, IPS and Application Control, Content Filtering Service and 24x7 Support with Software & Firmware Updates and Advanced Hardware Replacement.	1	$ 4.000,00	$ 4.000,00
01-SSC-7095	Stateful High Availability Upgrade (Licencias HA)	1	$600,00	$600,00
	Equipos remotos para la sucursal			
01-SSC-4890	**Sonicwall Firewall TZ 205 TotalSecure 1 Year** Comprehensive Gateway Security Suite includes - Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention and Application Firewall service, as well as Content Filtering Premium Services and 24x7 Support with Firmware Updates.	25	$ 600,00	$ 15.000,00
	Servicios de Implementacion			
SERV-001	Sonicwall Jump Start Service Implementacion de VPN Site to Site 25 sitios HA Internet y DSL Datos	1	$ 7.000,00	$ 7.000,00
	Proteccion de Correo			
EPCECE-AA-FP	**McAfee SaaS Email Protection & Continuity** LICENSE: Per User Email Account. Cloud-based product solution that provides inbound and outbound email security. **Filters inbound spam, phishing, malware and unwanted content**. Filters outbound malware and provides policy enforcement. **Email Continuity included to ensure continuous email access upon email server outages**. Virus filtering as part of malware filtering includes **3 layers: McAfee, WormTraq, and Commtouch Command Antivirus engines.**	1200	$10,04	$12.048,00
	Proteccion de Correo			
SERV-001	**McAfee Jump Start Service incluye** Configuracion Traspaso de conocimiento y puesesta a punto Entrenamiento formal por el fabricante en situ	1	$ 20.000,00	$ 20.000,00
	Servcios de Comunicaciones			
ISP-1	Servicio de Internet sincrono upgrade 10 a 60 MB CLARO	1	$ 40.000,00	$ 40.000,00
ISP-2	Servicio de Internet sincrono 60 MG Actual TRICOM	1	$ 35.000,00	$ 35.000,00
ISP-3	Servicio de Internet sincrono 60 MG Actual WIND	1	$ 30.000,00	$ 30.000,00

Servcios Rack Spacce Cloud				
HOST-EXCH	Microsoft Exchange Cloud Enviroment Annual	1200	$9,00	$10.800,00
HOST- SQL	Microsoft SQL Server Cloud per Database Instance Annual	1	$3.500,00	$3.500,00
HOST- WEB	Microsoft Web Server Cloud Annual	1	$2.500,00	$2.500,00
HOST- INFRA	10 Virtuak Microsoft Windows Server Annual	1	$15.000,00	$15.000,00
			Subtotal	$178.000,00
			Impuestos	$32.040,00
			Total	**$210.040,00**

Precios en Dollares

Encuesta sobre la calidad de servicios que brinda el departamento de TI a la empresa

1. Considera usted que nuestros sistema de gestión es muy complicado?

- ○ Si
- ○ No

2. Cada cuanto tiempo reporta problemas de duplicidad de información del sistema?

- ○ Diario
- ○ Semanal
- ○ Mensual

3. Como usted evalúa la velocidad de acceso a nuestra aplicacion de finanzas?

- ○ Malo
- ○ Bueno
- ○ Regula

4. Usted utiliza frecuentemente los servicios de nuestra intranet ?

- ○ Siempre
- ○ Algunas Veces
- ○ Casi nunca
- ○ Nunca

5. Considera que el servicio de correo es vital para su trabajo?

- ○ Si
- ○ No

6. Como usted evalúa el acceso al servicio de correo?

- ○ Bueno
- ○ Regular
- ○ Malo

7. Como usted evalúa el acceso a los servidores de archivos?

- ○ Bueno
- ○ Regular
- ○ Malo

8. Considera que el servicio de internet es vital para su trabajo?

- ○ Si
- ○ No

9. Como usted evalúa la velocidad del servicio de internet ?

- ○ Bueno
- ○ Regular
- ○ Malo

10. Por cuales medio le gustaría comunicarse en la empresa si estuvieran disponibles?

- ☐ Chat
- ☐ Correo
- ☐ Telefono

Listo