Universidad Siglo 21

Trabajo Final de Graduación

Licenciatura en Informática

Proyecto de Aplicación Profesional (PAP)

Computación en la nube, controles de seguridad

´

Pablo Pi

VINF02602

Fecha: 13/02/2018

Docente: Ing. Adriana Perez

Abstract/ Resumen

Cada vez más y más empresas están subiendo sus infraestructuras tecnológicas a la nube. Este nuevo paradigma tecnológico es muy atractivo debido a que es una alternativa que brinda grandes beneficios a nivel de los costos y de la gestión, pero a su vez introduce en las empresas nuevos desafíos en materia de seguridad de la información muy diferentes a los presentados por las infraestructuras clásicas, como podremos comprobar en el desarrollo de este trabajo. Utilizar esta tecnología implica desde el inicio un cambio radical ya que los datos no sólo dejan de estar en el entorno cerrado de la empresa para pasar a residir en un tercero, sino que además por las características propias de esta tecnología estarán compartiendo recursos como procesadores, discos y memorias con el resto de los clientes.

Es el objetivo del presente trabajo definir cuáles son los controles de seguridad de la información que deberían ser implementados por la empresa si quiere adoptar esta tecnología en forma segura. Para identificar estos controles se llevará adelante un análisis de riesgos para entender los riesgos a los que se expondrá la empresa en este nuevo ámbito y así poder determinar cuáles son los controles más apropiados de acuerdo a las necesidades de la empresa. Todo este trabajo será guiado por la serie de normas ISO/IEC 27000 sobre seguridad de la información junto con la guía COBIT (Objetivos de Control para Información y Tecnologías Relacionadas) de ISACA (Asociación de Auditoría y Control de Sistemas de Información) sin perder de vista los objetivos del negocio.

Every day more and more companies are uploading their technological infrastructures to the cloud. This alternative offers great benefits in terms of cost and management; however, this alternative introduces new challenges in information security very different from those presented by the classic infrastructures, as we can notice during the present thesis work. The use of this kind of technology implies from the very beginning a radical change as data are no longer in the company´s close environment to reside on a third-party company and furthermore, due to the intrinsic characteristics of this technology, resources will be shared (i.e. processors, disks, memories) with the rest of the third party´s clients.

The objective of the present work is to analyze the risk to what the company will become exposed in this new area and to design the information security controls necessary to maintain a safe environment. To identify such controls, a risk assessment will be carried out to understand the risk that the company can be exposed in this new environment and so that to be able to determine which are the most proper controls per the company needs. The guidelines for the whole work is ISO/IEC 27000 standards – security information and COBIT (Control Objectives for Information and related Technology) from ISACA (Information Systems Audit and Control Association), always considering the objectives of the business.

Tabla de contenido

Tabla de imágenes

Título

Computación en la nube, controles de seguridad.

Introducción - Marco de referencia institucional

Kantar IBOPE Media es una empresa dedicada a la investigación de medios de comunicación en América Latina que proporciona a sus clientes información para la toma de decisiones sobre todos los aspectos relativos a la medición, el monitoreo y la planificación de medios.

IBOPE (Instituto Brasilero de Opinión Pública y Estadística) originalmente es una empresa privada brasilera creada en 1942 por el Sr. Auricélio Penteado. Dedicándose primeramente a la medición de audiencia de radio y posteriormente extendiendo sus estudios a otros medios (TV, Cine, Gráfica y Vía Pública). Durante más de 50 años IBOPE ha ido creciendo como una empresa líder en su rubro extendiendo su operación dentro del mercado latinoamericano hasta lograr presencia en 15 países. En 2015 pasa a llamarse Kantar IBOPE Media tras su adquisición por parte del grupo Kantar Media y de esta manera se incorpora a un conglomerado de empresas dedicadas a la investigación de mercado que operan en más de 60 países alrededor del mundo. Kantar IBOPE Media cuenta con aproximadamente 3.500 colaboradores.

Kantar Media ha llevado adelante en estos últimos años un proceso de crecimiento por adquisición de otras empresas. Esto ha provocado que en muchos casos existan áreas, tareas y recursos duplicados, triplicados y en ciertos casos multiplicados por varias veces.

Un claro ejemplo de esta problemática es el de la infraestructura tecnológica y puntualmente la multiplicidad de centros de cómputos. Cada empresa adquirida o bien contaba con uno o tenía contratado un servicio de alojamiento de servidores en un centro de cómputo externo.

Dentro de este contexto, en 2016 la compañía inicia un proceso de reingeniería de toda su infraestructura con la finalidad de consolidar sus múltiples centros de cómputos. Tras

finalizar este trabajo se toma la decisión estratégica de migrar los centros de cómputos a un modelo de *cloud computing*.

Este tipo de ambientes seducen a las compañías porque plantean desde los casos de estudio, grandes ahorros en los costos de tecnología de las compañías o gobiernos. Por ejemplo, el Estado de California estimó este ahorro en u$s5,5 millones en el plazo de 5 años por su migración del correo electrónico a la plataforma de Gmail (Gartner, 2011). Sin embargo, los usos de estas tecnologías plantean grandes desafíos muchos de los cuales todavía no han sido resueltos sobre todo para el campo de la seguridad de la información.

En relación a este proyecto es necesario desde mi función de Oficial de Seguridad de la Información evaluar y desarrollar un programa de seguridad acorde que permita acompañar este cambio. Para esto es necesario identificar las mejores prácticas de seguridad existentes que apliquen a los servicios que se vayan migrando y definir los controles apropiados.

En el caso puntual de este trabajo, se analizarán las necesidades de seguridad mediante un análisis de riesgos realizado según la metodología presentada en norma de Gestión de Riesgos de Seguridad de la información: ISO/IEC 27005:2011, para aquellos servicios que se vayan a migrar o implementarse en la nube, de forma tal que se obtenga una matriz de controles basados en la norma Código de prácticas para la gestión de la seguridad de la información: ISO/IEC 27002:2013 y la guía de buenas prácticas COBIT *(Control Objectives for Information and related Technology* u Objetivos de Control para Información y Tecnologías Relacionadas) con el objeto de que los mismos sean implementados para lograr un ambiente seguro y que cumpla tanto con las políticas de la empresa como con las normas que regulan a la industria.

Formulación de la Problemática

¿Cómo se puede controlar la seguridad de los activos de la información que se encuentran en la nube de forma que los mismos alcancen un nivel de protección similar a los servicios que son administrados por personal de la empresa y alojados en un centro de cómputos propio?

Justificación

Debido a la decisión de la empresa de migrar a un entorno de computación en la nube, se hace necesario desde el campo de la seguridad informática acompañar dicho proyecto para lograr niveles apropiados de seguridad en este tipo de ambientes.

Dada las necesidades de optimización de costos sumados a beneficios como implementaciones rápidas, fácil escalabilidad de los recursos, alta disponibilidad, entre otras bondades, la empresa encuentra en este nuevo paradigma, una solución a muchos de sus problemas tecnológicos.

Este cambio va a impactar de lleno en el área de seguridad informática dadas sus implicancias ya que los servicios que hasta ahora están alojados en servidores propios dentro de los centros de cómputos de la compañía y que además son administrados por empleados de la empresa dentro de un ambiente cerrado y controlado pasarán a residir en el centro de cómputos de un tercero, en servidores que son propiedad de ese tercero, que además se compartirán recursos (procesadores, memorias, discos, etc.) con otros clientes, sin dejar de tener en cuenta que estos servicios ahora serán accesibles desde internet y que la administración de esa infraestructura será realizada por los técnicos del proveedor del servicio en la nube, sólo por mencionar algunos de los cambios más importantes. Todos estos cambios generan riesgos que se irán describiendo y evaluando en forma minuciosa en las siguientes secciones y hace que el área de seguridad informática deba adaptarse para poder acompañar y permitir que los beneficios de este tipo de tecnologías puedan ser utilizados de manera segura por la empresa. Han sido tantos y tan rápidos los cambios en este ámbito que todavía existen muchos desafíos que aún no han sido resueltos.

La computación en la nube continúa creciendo, sumando servicios, prestaciones y disminuyendo costos por lo que su uso seguramente se ha de seguir expandiendo.

Por todo esto la empresa necesita encontrar una manera de abordar los nuevos problemas que genera este cambio, teniendo siempre en cuenta sus necesidades de seguridad y las del

entorno en el cual realiza sus negocios. Más adelante en el apartado *Cloud Computing* dentro marco teórico se enumeran de forma detallada los principales problemas que deben enfrentar las empresas en este tipo de ambientes.

No existe una formula única que pueda ser aplicada en todos los casos inclusive tratándose de la misma empresa es posible que según las características del servicio que vaya a implementar varíen las necesidades de seguridad de la información.

Objetivo general del proyecto

Frente al uso de esta nueva tecnología se plantean nuevos desafíos en el ámbito de la seguridad de la información. En general, para aquellas compañías que como Kantar IBOPE Media, la información se encuentra entre uno de sus activos más importantes y sobre todo cuando tienen un marco normativo que cumplir, sienten que, con la adopción de este nuevo paradigma, se está poniendo en riesgo el control de sus activos de información.

Para identificar cuáles son estos cambios, se llevará adelante un análisis de riesgos en base a la norma de Gestión de Riesgos de Seguridad de la información: ISO/IEC 27005:2011. Además, y con el objetivo de administrar los riesgos que se identifiquen se definirá una matriz con los controles de seguridad de la información para ámbitos de *Cloud Computing* sobre la base de la norma Código de prácticas para la gestión de la seguridad de la información: ISO/IEC 27002:2013 y la guía COBIT de ISACA. De esta manera, quedarán identificadas las prácticas de seguridad de la información que deben ser implementadas para dar cumplimiento a los requisitos de seguridad de la información enunciados en las políticas internas de la empresa y las normas que regulan su actividad.

Objetivos específicos del proyecto

A continuación, los objetivos específicos del proyecto:

- Dentro del ámbito de este proyecto se evaluarán los riesgos a los que está expuesto un servicio que se migra o implementa en un modelo de servicios *cloud*.

- Identificar los requisitos de cumplimiento en materia de seguridad de la información en políticas internas, legislación, normas y estándares de mercado.
- Definir los controles de seguridad de la información que deben ser implementados a través del diseño de una matriz de controles.

Límite

El proyecto abarca la selección e implementación de los controles de seguridad de la información necesarios, basados en la norma ISO/IEC 27002:2013 y COBIT, para mantener un nivel apropiado de seguridad en el entorno *cloud* contratado por la empresa.

Alcance

El entorno de *cloud computing* de la Softlayer de IBM para los servicios de la filial de Argentina contratados por Kantar IBOPE Media.

No Contempla

El presente trabajo no contempla los controles que no sean propios de un ambiente de *cloud computing* basados en las normas utilizadas como referencia en el presente trabajo.

Marco Teórico

La tecnología de la información desde sus inicios no ha dejado de crecer, lo ha hecho a pasos agigantados y cada vez más rápidos, sobre todo desde la irrupción de las computadoras personales en el ámbito empresarial. La seguridad informática ha acompañado este desarrollo y su rol ha ido cobrando una importancia fundamental desde que el uso de la tecnología ha invadido todos los ámbitos de la vida moderna (Portantier, 2012). En menos de 30 años, pasamos de pensar que la computación se encontraba restringida a ámbitos cerrados en el que la única computadora era un Mainframe al que si un operador quería acceder sólo lo podía hacer a través de una terminal boba (Harris, 2012), a nuestro actual mundo híper conectado en el que nuestro teléfono celular nos informa 30 minutos antes de irnos del trabajo cuánto tiempo vamos a tardar en llegar a casa con una exactitud increíble.

Estos cambios en la tecnología deben ser acompañados necesariamente por la seguridad de la información porque seguramente nuestras vidas se verán afectadas como resultado de los mismos; para comprender mejor como podrían afectar nuestra vida, pensemos por un instante cuáles serían las consecuencias de realizar tan solo un cambio sin llevar adelante previamente los controles apropiados en el sistema informático que controla el monitoreo de una unidad de cuidados intensivos en un hospital ¿Cuántas vidas estarían en peligro? Ejemplos simples no permiten entender el importante papel de la seguridad en determinados ámbitos.

A lo largo de todo este tiempo hemos pasado de esos ambientes cerrados monolíticos a arquitecturas cada vez más heterogéneas y cada vez más interconectadas. Lo que hace que la seguridad de la información se deba reformular para hacer frente a cada cambio.

Todo tiene un inicio y en el caso de la computación en la nube este parece estar en las ideas que presentaron los informáticos estadounidenses Joseph Carl Robnett Licklider y John McCarthy en los años sesenta. El primero pensó en la idea sobre un concepto que llamó "red de computadoras intergaláctica" (Licklider, 1963) cuya idea central era que todo el mundo pudiese estar interconectado y poder acceder a los programas y datos sin importar donde estuviera. Mientras que McCarthy presentó el concepto en un discurso que dio en 1961 en el MIT (*Massachusetts Institute of Technology*) donde mencionó que “Algún día la computación podrá ser organizada como un servicio público" (Garfinkel, 2011) similar a cualquier otro servicio público como el agua o energía. Pero si bien ellos fueron de los primeros que pensaron en este concepto, el mismo no tuvo un nombre concreto hasta 2006 cuando se publicó en la revista *Wired* un artículo de George Gilder llamado “Las fábricas de información” en el que se usó el término *Cloud Computing* por primera vez. Estos fueron los puntapiés iniciales de los actuales servicios de *cloud computing* ofrecidos por casi todos los gigantes tecnológicos. Estos son servicios muy atractivos por lo que han llevado a la mayoría de las empresas a evaluarlos y adoptarlos casi masivamente por sus bajos costos, sumados a la posibilidad de provisionar servicios rápidamente y con poco esfuerzo de administración. Sin embargo, esta adopción requiere que la seguridad informática se adecue para soportar estas soluciones haciéndolas seguras para hacer frente a los riesgos inherentes a este tipo de

tecnología que son en algunos casos radicalmente distintos a los que la empresa venía enfrentando. Un claro ejemplo que nos permitirá comprender mejor lo mencionado previamente, lo podemos ver cuando entendemos que por sus características intrínsecas en un entorno *cloud* los datos de los múltiples clientes comparten recursos como procesador, memoria y disco. Esto no ocurría cuando esos mismos datos se encontraban en un servidor propiedad de la empresa. Pensemos en la complejidad técnica que implican las medidas que permiten aislar los datos de cada cliente y lo difícil que es controlar esto para la empresa que contrata el servicio en la nube.

El impulso dado por muchas organizaciones como el NIST (Instituto Nacional de Normas y Tecnología de Estados Unidos), la ISO (Organización Internacional para la Estandarización), el ISC2 (Consorcio internacional de Certificación de Seguridad de Sistemas de Información) y la CSA (*Cloud Security Alliance*), entre otras, generando normas, guías, investigaciones y certificaciones es una muestra cabal de la importancia que ha cobrado el uso de esta tecnología dentro de las organizaciones. No obstante, todos estos estándares, guías y conocimientos deben ser estudiados en profundidad para encontrar la mejor manera de adaptarlos e incorporarlos en forma de controles que sean realmente efectivos y apropiados al momento de proteger los activos de información de una empresa determinada.

Actividad del cliente

La actividad principal de Kantar IBOPE Media es la medición de audiencias, es decir, mensurar el consumo real por tipo (televisión y radio), dispositivo y perfil demográfico.

Kantar IBOPE Media ofrece mediciones precisas e independientes de modo que sus clientes pueden monitorizar su inversión en contenidos, tomar decisiones sobre programación y maximizar los ingresos del tiempo de emisión. Estas mediciones ayudan también a los clientes en la toma de decisiones de inversión publicitaria.

Las mediciones de audiencia son realizadas mediante dos metodologías: *people meters* y cuadernillos.

El *people meter* es un dispositivo electrónico que se conecta al televisor y permite medir la audiencia en tiempo real registrando automáticamente el encendido y el cambio de canal, de cada uno de los miembros del hogar o sus visitas. Se encuentran instalados más de 2500 *people meters* que posibilitan medir la audiencia de TV Abierta y TV Paga en Buenos Aires, Córdoba, Mendoza y Rosario.

Ilustración 1 People Meter
Fuente: (Kantar IBOPE Media)

En el caso de la metodología de cuadernillos, la persona lleva un registro manual de su consumo de televisión y lo envía en forma periódica a la empresa para su cómputo. La metodología de cuadernillos es utilizada para medir la audiencia en Tucumán, Mar del Plata, Bahía Blanca, Santa Fe, Paraná, Río Negro y Neuquén.

T.I.C (Tecnología de la Información y Comunicación)

Cloud Computing

La computación en la nube o *cloud computing* es un paradigma mediante el cual distintas empresas ofrecen servicios de computación, generalmente basados en virtualización y en tecnologías distribuidas, que van desde simples aplicaciones hasta centros de cómputos

enteros y a los cuales se accede a través de internet con un pago que varía generalmente en función del uso (Mell y Grance, 2011).

Las arquitecturas de computación en la nube se caracterizan por ser:

- A demanda y autoservicio: el cliente puede aprovisionarse capacidad de cómputo en forma autónoma e incorporar mayores recursos si fuera necesario.
- *Pay-per-use or charge-per-use:* el cliente paga sólo por los recursos que utiliza. Los proveedores de servicios en la nube cuentan con la capacidad de medir automáticamente el uso de recursos. Dada esta capacidad de medición, es posible facturar al cliente por el uso de los recursos según distintas características, por ejemplo, almacenamiento, procesamiento, ancho de banda y cuentas de usuario activas.
- Disponibilidad, escalabilidad y flexibilidad: la cantidad o capacidad de los recursos contratados se pueden incrementar o disminuir según los requerimientos del cliente sin mayores inconvenientes, en forma transparente e incluso según el tipo de servicio de manera automática.
- Compartición de recursos (hardware, base de datos, memoria, almacenamiento, etc.): el proveedor de servicios utiliza sus recursos como si fueran un *pool* con los cuales atiende a múltiples clientes. Por citar un caso, en un momento dado un procesador físico puede estar prestando servicio a dos clientes en forma simultánea, la separación es lógica mediante un modelo *multi-tenant* (multi-propietario: sobre un único recurso operan múltiples clientes).

Hoy en día existe un catálogo muy extenso y variado de servicios de *cloud computing* que se ofrecen en el mercado y la mayoría de las empresas ya han empezado a utilizar este tipo de servicios en mayor o menor medida porque pareciera ser que ninguna se quiere quedar afuera de este cambio o perderse los beneficios que plantea este nuevo paradigma. Beneficios que mencionaremos más adelante.

El *cloud computing* se puede implementar de cuatro maneras:

- *Cloud* Pública: en este caso la nube pertenece y es administrada por empresas que la utilizan para ofrecer servicios *cloud* a otras empresas o personas individuales. Más

adelante detallaremos que tipo de servicios son ofrecidos. Algunos ejemplos de nubes públicas son *Amazon Elastic Compute Cloud (EC2), Softlayer de IBM, Sun Cloud, Google Cloud Platform y Windows Azure Services Platform*.

- *Cloud* Privada: en este modelo la nube pertenece y es administrada por una única empresa que brinda servicios a sus propias unidades de negocios. Se podría decir que este tipo de nubes tiene como ventaja un mayor nivel de seguridad y privacidad ya que los datos siguen estando en el ámbito de la empresa y, con ello, un mayor control. La mayoría de los casos de estudio indican que no son recomendables para empresas chicas o medianas por su alto costo.
- *Cloud* Híbrida: en este caso el modelo está formado por una base de *cloud* privada que incorpora e integra a su infraestructura servicios de *cloud* pública. Este modelo aprovecha lo mejor de los dos mundos. Esta implementación permite por un lado que las aplicaciones críticas del negocio y los datos sensibles queden dentro del ámbito controlado por la empresa (*cloud* privado) y mientras tanto incorporar el beneficio del uso del *cloud* público para implementar soluciones que necesiten ser escalables, tener elasticidad y que a su vez sean económicas.
- *Cloud* Comunitaria: la infraestructura de este tipo de nube está preparada para el uso exclusivo por parte de una comunidad específica de organizaciones que tienen objetivos similares en materia de requisitos de seguridad, o sobre consideraciones relacionadas con el cumplimiento normativo. En general, pueden ser propiedad administrada y operada por una o más de las organizaciones que integran la comunidad o incluso un tercero.

Por otro lado, los servicios de *cloud computing* se ofrecen principalmente bajo tres formatos:

- Plataforma como Servicio (*PaaS, Platform as a Service*): en esta modalidad son entornos preparados para el desarrollo de software. Se puede contratar un entorno con todas las herramientas necesarias para desarrollar e implementar una aplicación. Como por ejemplo sistemas operativos, motores de bases de datos, herramientas de diseño y desarrollo. Entre las principales ventajas de este tipo de servicios podemos destacar que se puede iniciar un proyecto de desarrollo de software sin tener que hacer grandes inversiones en hardware físico, no hace falta de expertos en infraestructura para

implementar y dar soporte, además permite el desarrollo de trabajo colaborativo en el caso de equipos que se encuentran físicamente distribuidos.

- Software como Servicio (*Saas, Software as a Service*): en este caso el proveedor de servicio deja disponible una instancia de una aplicación a través de la nube para que el usuario o empresa que contrató el servicio acceda al mismo por medio de internet. Claros ejemplos de este tipo de servicios son las herramientas de ofimática de Google o el servicio de correo de Office 365 de Microsoft. Se encuentran entre las principales ventajas de esta clase de servicios: el ahorro en costos de *hardware*, la fácil escalabilidad, que no requieren de largas y complejas implementaciones y que las aplicaciones son siempre accesibles desde cualquier lugar.
- Infraestructura como Servicio (*IaaS, Infrastructure as a Service)* consiste en entregar al cliente recursos informáticos en el formato de hardware virtualizado. Este concepto abarca servidores y redes. El modelo *IaaS* proporciona acceso a recursos informáticos ubicados en un entorno virtual llamado *cloud computing* por medio de una conexión a internet. Físicamente estos recursos provienen de múltiples servidores repartidos entre una gran cantidad de centros de cómputos propiedad del proveedor del servicio.

Los modelos de nubes y servicios detallados anteriormente están basados en las definiciones dadas por el NIST en su directriz 800-145 (Mell y Grance, 2011) y también en descripciones dadas por los distintos proveedores de servicios *cloud* en sus páginas *web* (ibm.com, 2018) (aws.amazon.com, 2018). Estas definiciones han sido adoptadas por todos los proveedores de la industria como un estándar.

Representación visual de la definición de la NIST del *cloud computing*

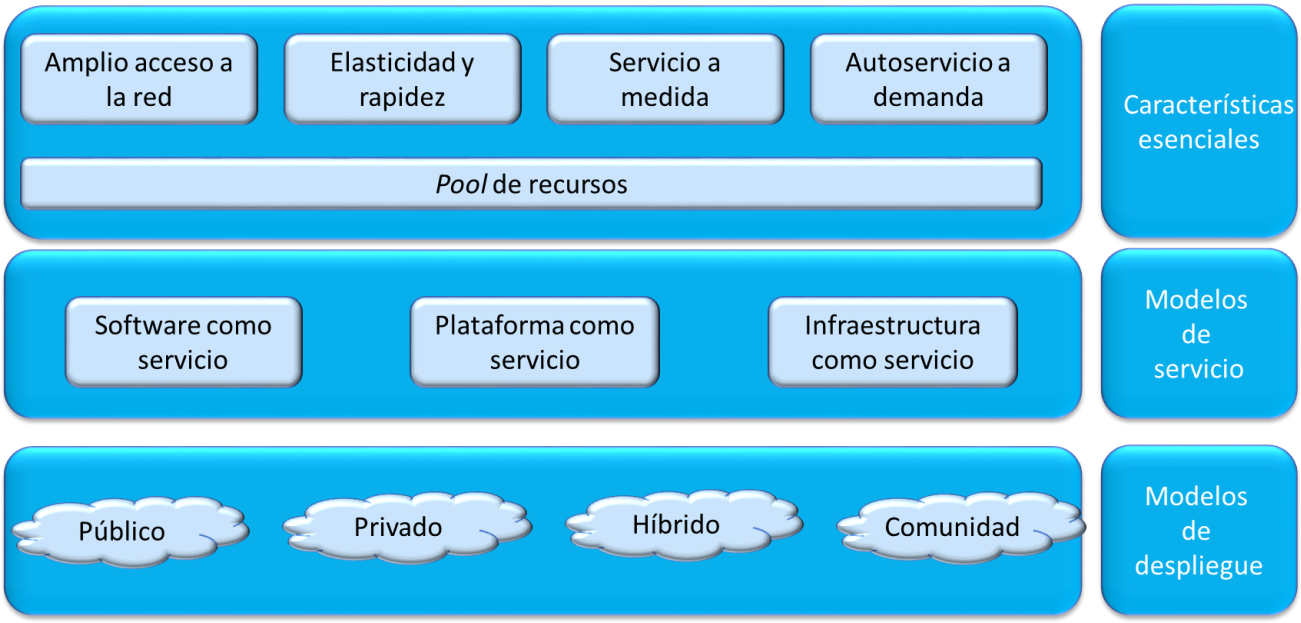


Ilustración 2 Modelos de *Cloud Computing*

Fuente: (Propia)

La computación en la nube también presenta ciertas ventajas en los aspectos relacionados con la seguridad de la información, como, por ejemplo:

- Escala: así como la gran escala en cuanto a los recursos de cómputo permite bajar los costos, en general las medidas de seguridad suelen ser más baratas cuando se aplican a gran escala. Muchas empresas que contratan los servicios en la nube no estarían en condiciones de implementar dentro de sus infraestructuras tecnológicas el mismo nivel de seguridad simplemente porque no cuentan con los recursos económicos ni el personal especializado para hacerlo.
- La seguridad como diferencial: si hoy en día para lograr el normal funcionamiento de una empresa, la misma necesita que se mantenga la confidencialidad, integridad y disponibilidad de su información para alcanzarlo, entonces seguramente la seguridad de la información sea una de las principales preocupaciones al momento de adoptar este tipo de tecnologías y hace que los proveedores de servicios busquen mejorar sus prácticas de seguridad y estar a la vanguardia como una forma de distinguirse de los

demás. Para poder demostrar este compromiso con las mejores prácticas muchos proveedores se certifican bajo alguna normativa relacionada. De esta forma, los clientes pueden conocer qué estándares de seguridad aplican las empresas proveedoras de servicios *cloud y* si tienen una certificación, qué entidad emitió el certificado y el alcance del mismo. Las siguientes son algunas de las certificaciones más importantes para proveedores de servicios en la nube (ENISA, 2007):

- *Certified Cloud Service - TÜV Rheinland*
- *CSA Self-Assessment - OCF Level 1*
- *CSA Certification - OCF Level 2*
- *CSA Attestation - OCF Level 2*
- *ISO/IEC 27001 Certification*
- *EuroCloud Star Audit Certification*
- *Service Organization Control (SOC) 1, 2 and 3*
- *Leet Security Rating Guide*
- *Payment Card Industry Data Security Standard v3*
- *Cloud Industry Forum Code of Practice*

- Interfaces Estandarizadas: los proveedores de servicios *cloud* ofrecen en general interfaces abiertas y estandarizadas de manera que sea sencillo interconectar la nube con diversos servicios o herramientas de seguridad.
- Auditoría: dado que este tipo de arquitecturas están basados en virtualización es relativamente sencillo generar imágenes forenses y resguardar las originales sin interrumpir el servicio. Referido también al tema de las auditorías nos encontramos con la solución a un problema habitual en las empresas que es la falta de registros de eventos o *logs* de transacciones por no contar con espacio de almacenamiento suficiente que permita un resguardo de los mismos por el tiempo que sea necesario según los requerimientos normativos que la empresa deba cumplir. Cuántas más fuentes de registros de eventos o *logs* se deben controlar y cuánto más detalle se requiere de las actividades realizadas, mayor será el volumen de información que se generará y por tanto mayor será la necesidad de espacio de almacenamiento disponible requerido. Otra

vez la escala juega a favor de la seguridad, en este caso permitiendo que la empresa contrate más espacio de disco a medida que se lo necesite sin tener que tener una capacidad ociosa y en general a un menor costo.

- *Hardening*: dentro de los entornos virtuales es mucho más fácil para los proveedores de servicios aplicar las configuraciones de seguridad y parches a las máquinas virtuales por defecto y configurar en forma segura los módulos de *software* que ofrecen en sus tiendas virtuales. En los ambientes virtuales es común contar con lo que se llama imagen base que no es más que una preinstalación de un sistema operativo con sus configuraciones básicas. Esta imagen base se actualiza constantemente para que cada nueva instancia de la misma que se provisiona al cliente cuente con las últimas actualizaciones y todas las configuraciones de seguridad necesarias.

Así como la computación en la nube presenta ventajas desde el punto de vista de seguridad también presenta riesgos. En ese sentido basados en los análisis y estudios llevados adelante por varias de las instituciones más importantes dedicadas a la seguridad como el ISC2 (Consorcio internacional de Certificación de Seguridad de Sistemas), ISACA (Asociación de Auditoría y Control de Sistemas de Información) , NIST (Instituto Nacional de Normas y Tecnología, USA), CSA (Cloud Security Alliance) es que OSWAP (Proyecto Abierto de Seguridad de Aplicaciones Web) ha desarrollado y publicado su *top ten* de riesgos de seguridad en la nube. Los cuales se presentan brevemente a continuación (OSWAP, 2018):

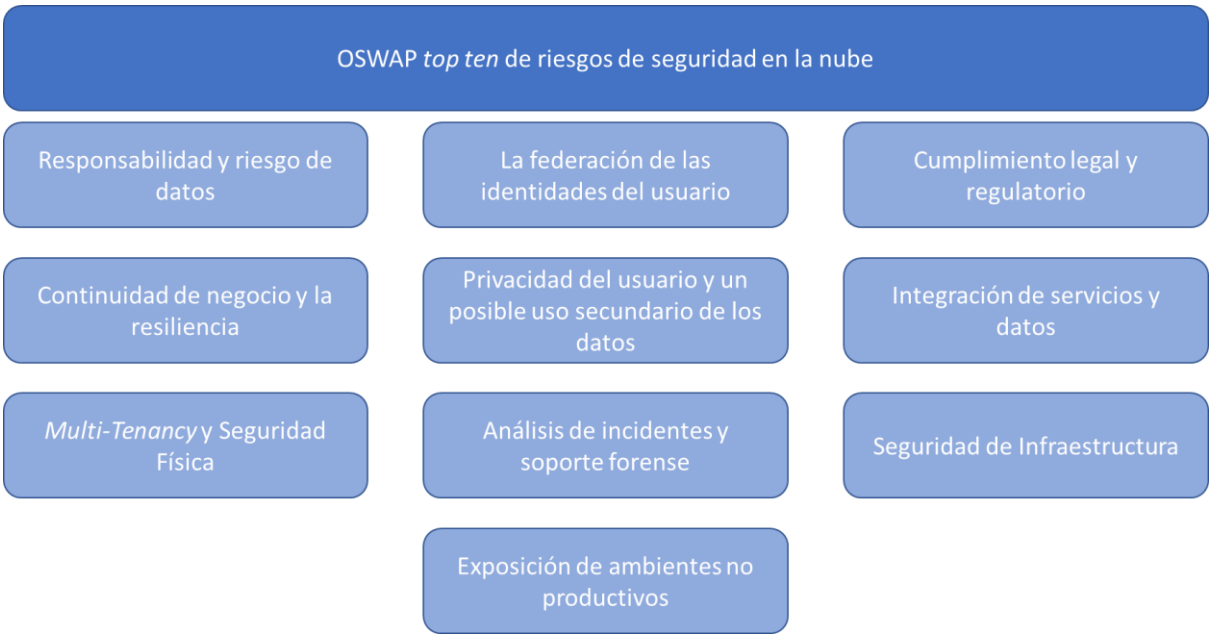


Ilustración 3 OSWAP *Cloud Risk Top Ten*

Fuente: (Propia)

1. Responsabilidad y riesgo de datos: en un entorno clásico donde el centro de cómputos es propiedad de la empresa, determinar la responsabilidad en materia de seguridad es relativamente sencillo; sin embargo, al pasar a un entorno *cloud*, establecer dicha responsabilidad empieza a ser más difícil de determinar. Si pensamos el centro de cómputos en capas, podemos decir que dentro del mismo tenemos aplicaciones, servidores web, bases de datos, procesamiento, almacenamiento y redes. Dentro de un entorno *cloud*, dependiendo el tipo de servicio contratado, los límites entre cada capa pueden llegar a ser difíciles de establecer claramente. En el caso de los datos, surgen riesgos relativos a la propiedad de los datos y su protección. Sumado a esto en muchos de los casos ni siquiera se puede establecer la ubicación física de los datos porque los proveedores cuentan con múltiples locaciones radicadas en diferentes sitios.
2. La federación de las identidades del usuario: es importante que las empresas puedan mantener el control sobre las identidades de los usuarios para contar con trazabilidad de las actividades que realizan.
3. Cumplimiento legal y regulatorio: el simple hecho de que los datos estén ubicados en un país diferente al que se encuentra radicada la empresa hace que los mismos estén sujetos a dos legislaciones distintas y eso sólo suponiendo que las redes que

interconectan a la empresa con el proveedor no pasen por ningún otro país intermedio. Esta diferencia de legislaciones puede llevar fácilmente a un incumplimiento por parte de la empresa. Por ejemplo, la legislación europea con su RGPD (Reglamento de Protección de Datos de La Unión Europea) (eugdpr.org, 2018) es muy celosa en todo lo referido a privacidad en tanto que en Estados Unidos; gracias a la llamada Ley Patriota (justice.gov, 2018) la mayoría de las agencias federales de seguridad de ese país tienen permitido el acceso a casi cualquier información por lo que cualquier empresa radicada en Europa no podría contratar un servicio en la nube cuyos datos residan o pasen por Estados Unidos.

4. Continuidad de negocio y la resiliencia: cuando se contrata un servicio de *cloud computing* la empresa delega el control de la continuidad de ese servicio en el proveedor. Si esto no es tenido en cuenta al momento de la contratación del servicio es posible que se presenten problemas si los procesos del proveedor no cumplen con los requisitos de negocio de la empresa.
5. Privacidad del usuario y un posible uso secundario de los datos: hay un riesgo en el uso inapropiado por parte del proveedor de servicios *cloud* de la información que almacena de sus clientes.
6. Integración de servicios y datos: los datos en este modelo deben obligatoriamente atravesar internet para conectar a la empresa con el proveedor de servicios. Dependiendo de cómo este hecha esta integración podría tener un impacto negativo en la seguridad de la información.
7. *Multi-Tenancy* y Seguridad Física: un entorno *cloud* el termino *Multi-Tenancy* se utiliza para indicar que se comparten recursos y servicios para ejecutar instancias de software que sirven a múltiples clientes. Esto quiere decir que los recursos físicos almacenamiento, redes, etc., pueden ser compartidos por varios clientes en forma simultánea. A modo de ilustración, en la siguiente imagen podemos ver como un mismo proveedor atiende a tres clientes distintos (con políticas de seguridad distintas, niveles de servicios distintos e incluso con una facturación por servicios distinta) con la misma infraestructura física.

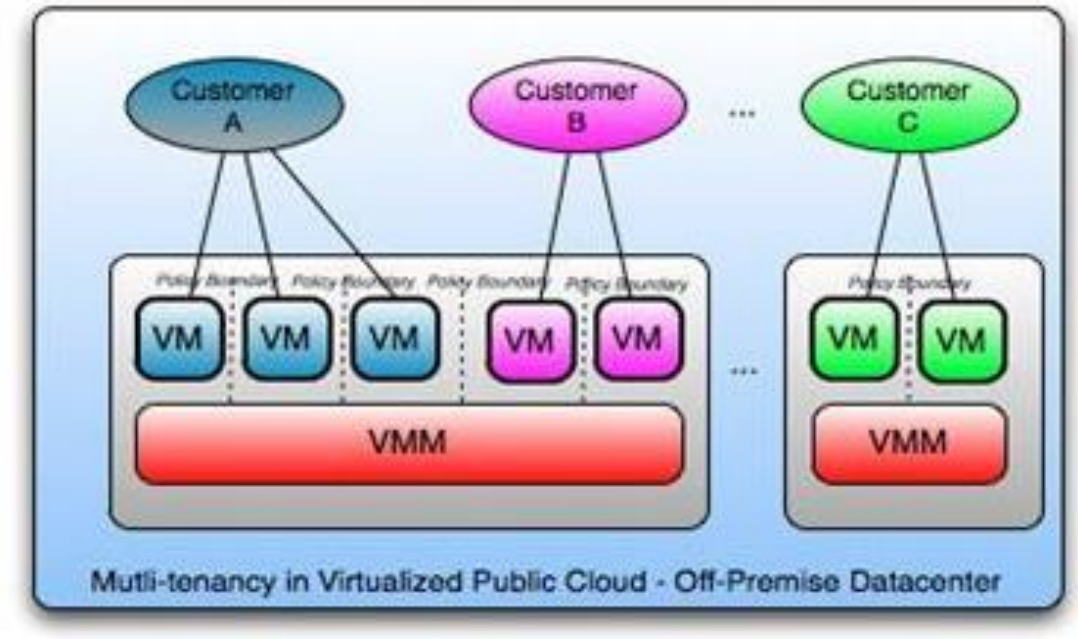


Ilustración 4 ***Multi-Tenancy***

Fuente: (*Cloud Computing Alliance*)

8. Análisis de incidentes y soporte forense: dado que los servicios en la nube en general siguen un esquema de computación distribuida, al momento de analizar un incidente puede hacerse muy difícil la recolección de información ya que la misma se puede encontrar en muchos sitios geográficamente separados. En este caso volvemos a encontrarnos con el problema de la transnacionalidad y las diferentes legislaciones aplicables.
9. Seguridad de Infraestructura: las fallas de seguridad a nivel de infraestructura afectan la seguridad de los datos que ésta soporta. Errores como: configuraciones por defecto, falta de actualizaciones, puertos innecesarios abiertos, accesos administrativos inapropiados, entre otros, ponen en riesgo la seguridad de la información contenida en dicha infraestructura.

10. Exposición de ambientes no productivos: los ambientes utilizados para el desarrollo de software generalmente no cuentan con las mismas medidas de seguridad que los ambientes productivos. Mientras este tipo de ambientes estaba en el centro de cómputos, la empresa tenía el control total de lo que pasaba con la información contenida en ese ambiente. Cuando la empresa decide migrar este entorno a la nube hay un tercero (el proveedor y sus empleados) que puede acceder a esa información que, como se mencionó al principio de este trabajo, no siempre cuenta con el nivel apropiado de seguridad, pudiendo contener información sensible en aquellos casos en que las bases de datos no fueron sanitizadas correctamente para su uso en el ambiente de desarrollo.

Dentro del ámbito de este proyecto se evaluarán los riesgos a los que está expuesto un servicio que se migra a un modelo *cloud IaaS* (Infraestructura como Servicio) dentro de un esquema de nube híbrida de manera que se puedan definir los controles apropiados a implementar para dar cumplimiento a los requerimientos de seguridad de la información definidos en la norma ISO/IEC 27002:2013 y en la guía de buenas prácticas COBIT. La plataforma de servicio en la nube a ser evaluada es Softlayer de IBM.

Herramientas y Metodologías para Análisis de Riesgos

Desarrollado por la empresa brasilera Modulo, el software *Risk Manager Tool* es una herramienta que contiene base de datos de conocimientos basadas en las mejores prácticas de seguridad (SOX, PCI, ISO 27001, HIPAA, COBIT, ITIL, FISAP, FISMA, NIST 800-53a, FIPS 199, A 130 and DOD 8500.2) para evaluar riesgos. Estas bases de conocimiento contienen diversas vulnerabilidades y escenarios de riesgos que pueden ser aplicados a distintos procesos de análisis (modulo.com.br, 2018).

El Proyecto OSWAP (en inglés *Open Web Application Security Project*, en español Proyecto Abierto de Seguridad de Aplicaciones *Web*) tiene como objetivo crear conciencia sobre la seguridad en aplicaciones mediante la identificación de algunos de los riesgos más críticos que enfrentan las organizaciones. En 2017, esta organización publica la versión más

actualizada del listado con el *top ten* de vulnerabilidades y una guía para el tratamiento que se debe aplicar para resolver cada una de ellas (oswap.org, 2018). Adicionalmente publican una serie de herramientas que permiten controlar y evaluar cada una de las vulnerabilidades descriptas en el *top ten*. Estas herramientas se conocen bajo el nombre de OSWAP *Top Ten Testing Tools*. Por otra parte, también se había creado un equipo de trabajo para el proyecto OWASP Cloud-10. El objetivo de este proyecto era ayudar a encontrar la forma de equilibrio entre los riesgos de seguridad y la ventaja de costo que ofrece el modelo *Cloud*. Este proyecto hoy se encuentra discontinuado, pero los estudios realizados por el equipo de trabajo han dejado información muy valiosa en este aspecto (oswap.org, 2018).

Serie Normas ISO/IEC 27000

En este apartado daré una descripción general de las normas relativas a la seguridad de la información que comprenden la serie ISO/IEC 27000 con foco en la norma ISO/IEC 27002. Más adelante en la sección de Diseño Metodológico explicaré con mayor detalle la norma ISO/IEC 27005 sobre gestión de riesgos.

Dentro del presente trabajo se buscará aplicar, siempre que sea posible, las mejores prácticas en cuanto a seguridad de la información. Por lo que muchas veces se encontrará la referencia a alguna de las normas de la serie ISO 27000. Esta serie es un compendio de normas que contienen las mejores prácticas en seguridad de la información para desarrollar, implementar y mantener un sistema de gestión de la seguridad de la información (SGSI).

Estos estándares son desarrollados y publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC). Esta serie tiene su inicio en la norma británica BS 7999, publicada por el BSI (*British Standard Institute*) en 1995 con la idea de establecer una serie de controles de seguridad de la información que ayudarán a las organizaciones a gestionar de forma segura sus activos de información.

Posteriormente la ISO se basó en dicho documento para diseñar la norma ISO/IEC 17799 que fue publicada en el año 2000.

Para el diseño de los controles utilizaré la norma ISO/IEC 27002 que es la norma que contiene los controles a implementar para lograr una correcta gestión de seguridad. Esta norma cuenta con catorce dominios, treinta y cinco objetivos de control y ciento catorce controles. A continuación, se listan los dominios que conforman la norma:

- Políticas de Seguridad
- Organización de la Seguridad de la Información.
- Seguridad en los Recursos Humanos.
- Administración de Activos.
- Control de Activos.
- Seguridad Física.
- Seguridad en las Operaciones.
- Seguridad en la Comunicaciones.
- Sistemas de Información, Adquisición, Desarrollo y Mantenimiento.
- Relaciones con Proveedores.
- Administración de Incidentes de Seguridad.
- Aspectos de Seguridad de Información en Continuidad de Negocios.
- Cumplimiento Normativo.

Los estándares ISO 27000 publicados hasta la actualidad relacionados con el presente proyecto son (iso.org, 2018):

- ISO/IEC 27000 — Sistemas de gestión de la seguridad de la información: descripción general y vocabulario.
- ISO/IEC 27001 — Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información - Requisitos.
- ISO/IEC 27002 — Código de prácticas para la gestión de la seguridad de la información.
- ISO/IEC 27003 — Guía de implementación del sistema de gestión de la seguridad de la información.

- ISO/IEC 27005 — Gestión de riesgos de seguridad de la información.
- ISO/IEC 27013 — Guía sobre la implementación integrada de ISO / IEC 27001 e ISO / IEC 20000-1 (derivada de ITIL)
- ISO/IEC 27017 — Código de prácticas para controles de seguridad de la información basados en ISO/IEC 27002 para servicios en la nube
- ISO/IEC 27018 — Código de prácticas para la protección de la información de identificación personal (PII) en nubes públicas que actúan como procesadores de PII

COBIT 5

Otra herramienta metodológica que se utilizará para ayudar en la definición de los controles a implementar será COBIT (Objetivos de Control para Información y Tecnologías Relacionadas), el cuál es un marco de trabajo para el gobierno de las tecnologías de información diseñado por ISACA (Asociación de Auditoría y Control de Sistemas de Información) que "proporciona una serie de herramientas para que la gerencia pueda conectar los requerimientos de control con los aspectos técnicos y los riesgos del negocio" (isaca.org, 2018). Además "COBIT permite el desarrollo de las políticas y buenas prácticas para el control de las tecnologías en toda la organización" (isaca.org, 2018). Este marco de trabajo contiene las mejores prácticas para el gerenciamiento de tecnologías de la información recomendadas por los expertos. La misión de COBIT es "investigar, desarrollar, publicar y promocionar un conjunto de objetivos de control generalmente aceptados para las tecnologías de la información que sean autorizados (dados por alguien con autoridad), actualizados, e internacionales para el uso del día a día de los gestores de negocios (también directivos) y auditores" (isaca.org, 2018). COBIT fue lanzado por ISACA en 1996 y actualmente se encuentra vigente su versión 5. COBIT está desarrollado bajo cinco principios (ISACA, 2012):

- Satisfacer las necesidades de las partes interesadas.
- Cubrir la Organización de forma integral.
- Aplicar un solo marco integrado.
- Habilitar un enfoque holístico.
- Separar el Gobierno de la Administración.

Por medio de COBIT 5 las empresas logran construir un marco para facilitar el gobierno y la administración las tecnologías de información.

Escáner de Vulnerabilidades

Un escáner de vulnerabilidades es un programa diseñado para evaluar las debilidades de los servidores, sistemas informáticos, redes o aplicaciones. Básicamente, estos programas se utilizan para descubrir los puntos débiles o partes mal desarrolladas. Para llevar adelante las pruebas de vulnerabilidades sobre el entorno de computación en la nube se utilizará la herramienta de administración de vulnerabilidades de Qualys Guard en su versión SaaS (*Software as a Service* o *Software* Como Servicio). Esta herramienta permite el análisis sistemático de los activos de información en busca de vulnerabilidades que podrían comprometer la seguridad de los mismos. Qualys Guard permite administrar el ciclo de vida completo de la gestión de vulnerabilidades (qualys.com, 2018). En la sección Propuesta de Implementación se presentan mayores precisiones sobre cómo se encuentra instalada esta solución y su funcionamiento.

Sistema de Correlación de Eventos

Los sistemas de correlación de eventos comúnmente llamados SIEM por sus siglas en inglés (*Security Information and Evento Management*) son aplicaciones que permiten recolectar registros de eventos (*logs* en inglés) de diversas fuentes tales como servidores, aplicaciones, sistemas operativos, bases de datos, dispositivos de red, etc. y correlacionarlos con el fin de realizar un análisis de los mismos en busca de patrones de eventos que permitan detectar una actividad maliciosa (Harris, 2016). En grandes ambientes tecnológicos el uso de este tipo de herramientas facilita y hace posible la revisión de grandes volúmenes de información, tarea que de realizarse en forma manual resultaría prácticamente imposible de llevar adelante en forma eficaz. Kantar IBOPE Media ya cuenta con una solución de SIEM implementada mediante el *software* HP ArcSight Logger de Hewlett Packard (hp.com, 2018). Además, la administración de esta herramienta se encuentra tercerizada con la empresa Tempest Security Intelligence mediante un servicio llamado SOC (*Security Operation Center* o Centro de Operaciones de Seguridad). El SOC se ocupa de monitorear permanentemente el estado de la seguridad de la infraestructura tecnológica de la empresa mediante la información brindada

por el SIEM en un formato 7x24x365. De esta manera pueden detectar un ataque informático en tiempo real y darle una inmediata atención en conjunto con el equipo de seguridad de la información de la empresa. A continuación, se presentan los diagramas topológicos de la solución de SIEM y del SOC.

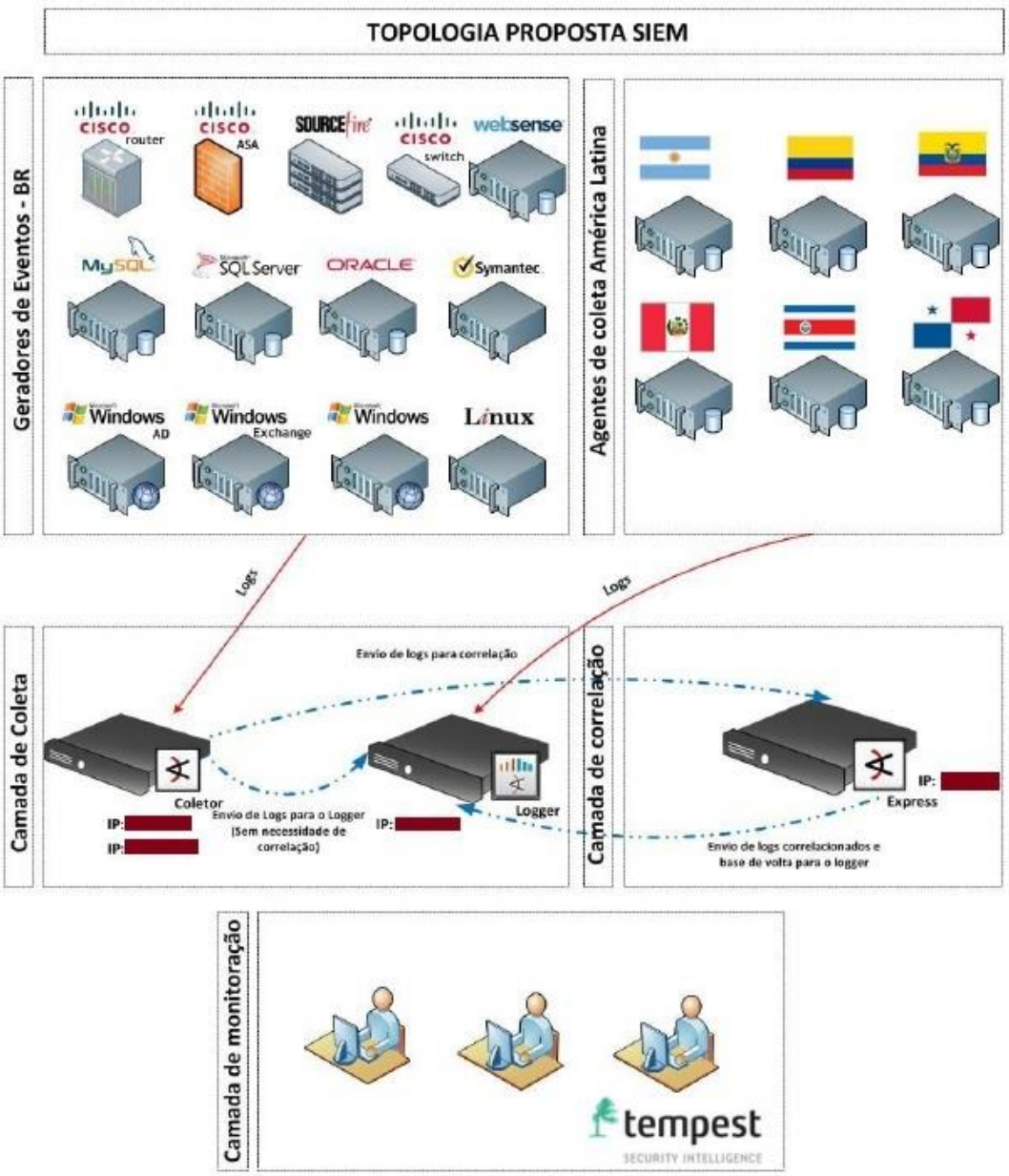


Ilustración 5 SIEM

Fuente: (Propia)

Como observamos en el esquema, los servidores, los dispositivos de red, las aplicaciones y las bases de datos generan *logs* que son colectados en el centro de cómputo de cada país por un servidor especial llamado agente de colecta. Estos, a su vez, transmiten la información recolectada a un conjunto de servidores ubicados en el centro de cómputos central ubicado en Brasil que se encarga~~n~~ de consolidar todos los registros recibidos mientras que otro servidor se ocupa de hacer la correlación de los mismos. Todo esto bajo el control de SOC externo que se encarga de monitorear las alertas que genera el SIEM. En la sección Propuesta de Implementación se presentarán mayores detalles de esta implementación y el funcionamiento del SOC.

Sistema de Administración de Contraseñas

Uno de los principales problemas de seguridad que enfrentan las grandes empresas es la gestión de las contraseñas críticas. A medida que se suman administradores se hace más difícil controlar quiénes utilizan y quiénes conocen estas contraseñas. Tengamos en cuenta que estas contraseñas en algunos casos permiten acceder a información muy sensible para la empresa y que si esa información se divulgase o fuera modificada de manera mal intencionada podría afectar seriamente los intereses de la empresa.

Un ejemplo que nos permite ilustrar una de las complejidades que se dan en la gestión de contraseñas ocurre en un hecho simple que ni siquiera requiere de malas intenciones, me refiero a cuando un administrador de red deja la compañía, él mismo conoce contraseñas que le permiten acceder, por ejemplo, a los 60 dispositivos de red de la empresa, incluso pudiendo acceder a muchos de ellos en forma externa. Entonces con cada salida de un administrador la empresa se vería obligada a modificar la contraseña de todos los dispositivos a los que esta persona tenía acceso.

Para ayudar con esta problemática existen varias herramientas en el mercado para administrar las contraseñas de una organización en forma segura. En el caso de Kantar IBOPE Media cuenta con la solución *Password Manager* Pro de ManageEngine. Esta herramienta funciona como un repositorio centralizado de contraseñas a la que cada usuario tiene acceso a las

contraseñas que le correspondan por su rol; de esta manera, la empresa puede trazar el uso de las mismas, además permite que tras el uso de una credencial de usuario se modifique en forma automática la contraseña de manera que no se pueda reutilizar. Otra funcionalidad con la que cuenta, es la posibilidad de grabar las sesiones de usuarios de manera que cuando otorga una contraseña grabe en formato de video toda la sesión del usuario mientras utiliza la contraseña que solicitó para una revisión posterior. Además, permite la generación de informes sobre quién ha tenido acceso a cada contraseña, en todo momento (manageengine.com, 2018). En las próximas imágenes podemos ver el menú principal cuando un usuario entra a la aplicación. En el mismo se encuentran los recursos a los que tiene acceso y haciendo simplemente *click* sobre el nombre del equipo se pueden ver los usuarios a los cuales tiene permiso. Otro *click* sobre el usuario y el sistema lo conecta al equipo seleccionado con el usuario elegido.

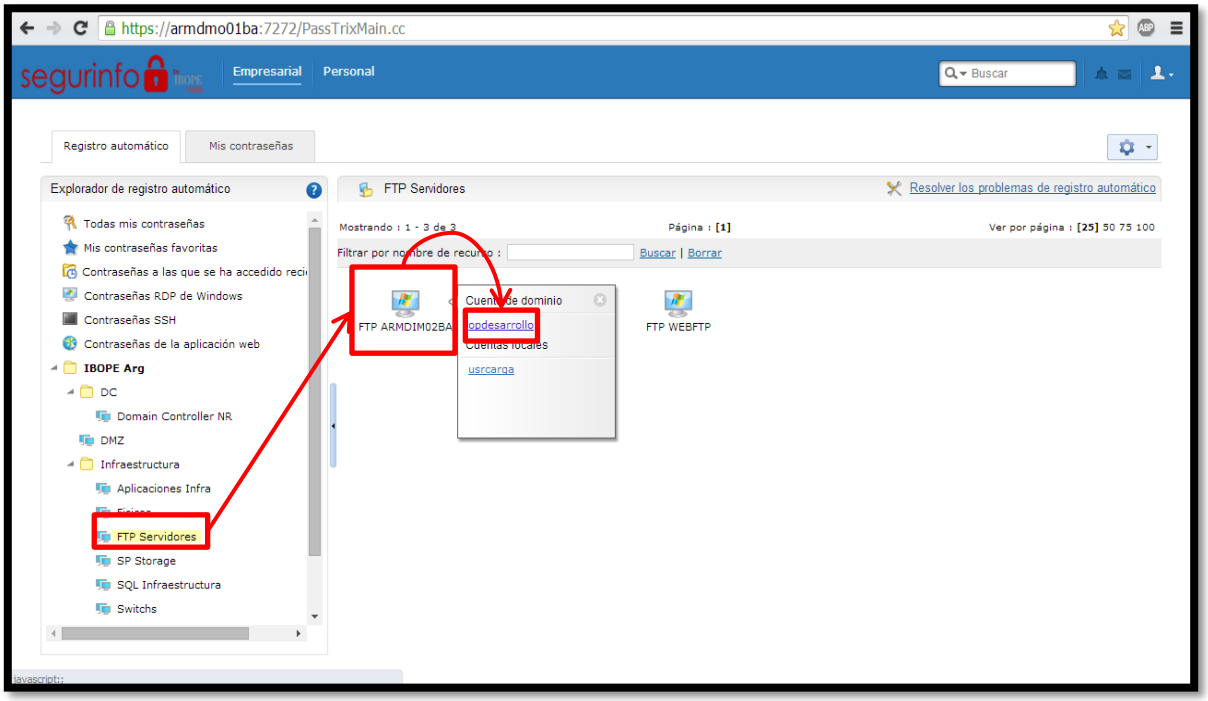


Ilustración 6 PMP 1

Fuente: (Propia)

Sistema de Monitoreo de Infraestructura

Uno de los pilares de la seguridad de la información es la disponibilidad. Dentro de este campo el término disponibilidad se entiende como el acceso de los recursos de datos a las

personas autorizadas y de manera oportuna (Harris, 2016). Si una empresa depende de su plataforma tecnológica para la toma de decisiones y la información no está accesible en el momento que se la necesita, difícilmente puede operar con eficiencia. Ni hablar en aquellos casos en el que todo el funcionamiento de la empresa está atado al normal funcionamiento de su infraestructura tecnológica. Una manera de tener un ambiente controlado y poder anticiparse a alguno de los problemas que se pueden presentar es tener implementado un sistema de monitoreo. Este tipo de sistemas permiten monitorear el estado de los servidores, dispositivos de red, controlar el uso de los procesadores, memorias, discos, servicios y aplicaciones entre otras cosas y emitir alertas en caso de que determinados umbrales sean superados. De esta manera, si un disco se está quedando sin espacio o un servidor está utilizando por períodos prolongados casi toda la memoria disponible en un servidor el administrador de la red puede tomar decisiones que eviten la ocurrencia de un incidente a futuro. En el caso de Kantar IBOPE Media este monitoreo es realizado por medio de la herramienta OpManager de ManageEngine (manageengine.com, 2018). Para realizar este monitoreo la empresa ha implementado un NOC (Network Operation Center o Centro de Operaciones de Red) en las oficinas de San Pablo, Brasil. En este centro, un equipo de ingenieros se ocupa de controlar 7x24x365 el sistema de monitoreo y atender las alertas que el mismo emite. En la próxima imagen podemos ver una de las pantallas de monitoreo, en este caso se trata de un servidor y podemos ver información sobre la disponibilidad del equipo, el estado del procesador, la memoria y el espacio en disco, entre otros detalles técnicos que permiten en este caso evaluar el estado del servidor.

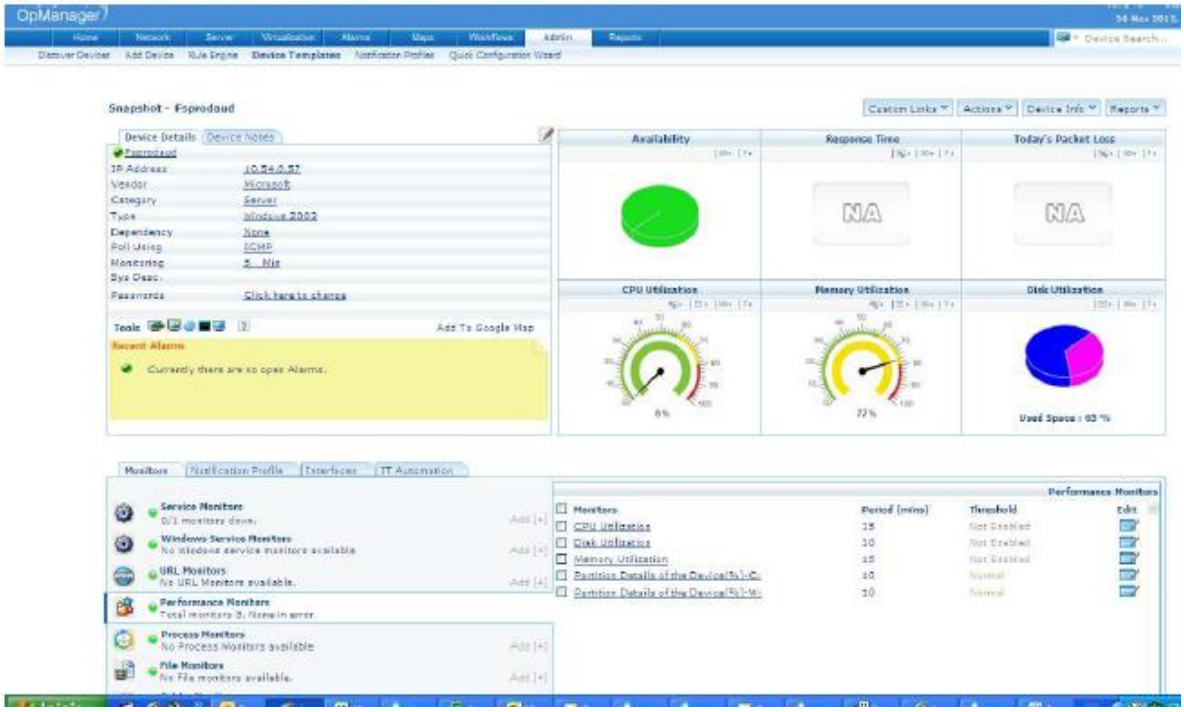


Ilustración 7 OpManager

Fuente: (Propia)

Federación de Identidades

Los sistemas de federación de identidades permiten gestionar en forma centralizada los usuarios de una organización cuando ésta posee múltiples y heterogéneos sistemas los cuales poseen, cada uno, su sistema propio de gestión de usuarios. Estos sistemas permiten crear relaciones de confianza entre todos los sistemas que posee la empresa de forma que cuando un usuario es dado de alta en la red, dependiendo de los roles que se le habilite, podrá tener acceso a todos los sistemas de la empresa que su perfil requiera siempre con el mismo usuario y contraseña. En este caso se utilizará el sistema de federación de identidades que ya trae la plataforma del servicio en la nube contratado. A continuación, se presenta un diagrama que muestra cómo trabaja esta solución.

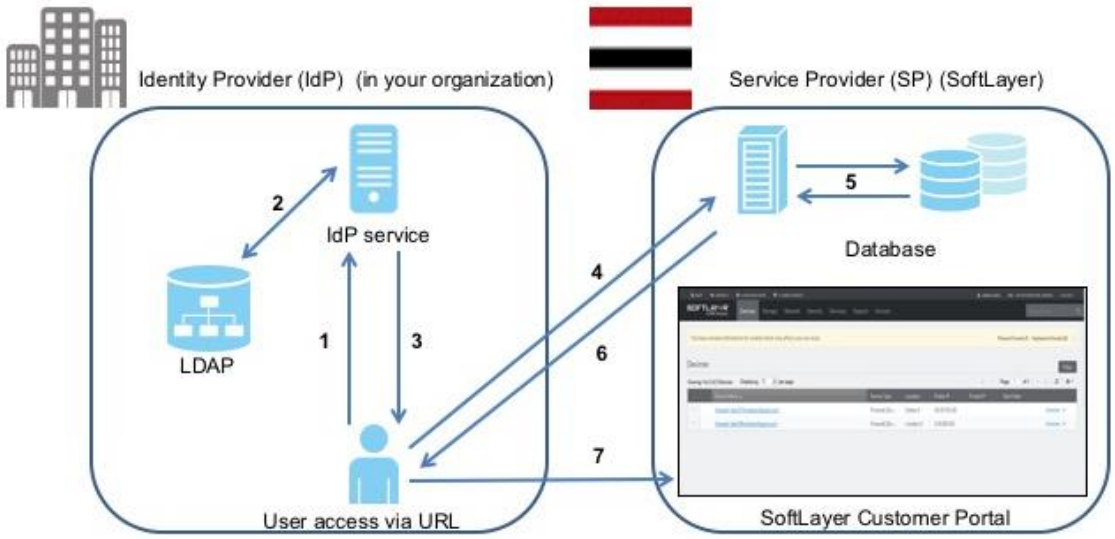


Ilustración 8 Federación de Identidades

Fuente: (softlayer.com)

Si seguimos el diagrama observamos que en el primer paso el usuario inicia sesión en un entorno web, éste se conecta con el servicio de identidades (indicado en el diagrama con las siglas IdP). En el segundo paso este servicio autentica al usuario contra la base de datos centralizada y responde en el paso tres. En caso que la autenticación haya sido exitosa esa respuesta es enviada por el servicio de identidades en el paso cuatro a la plataforma de Softlayer la cual valida las credenciales en el paso cinco y permite el acceso del usuario a la aplicación web, pasos seis y siete (softlayer.com, 2018)

Competencia – Proveedores de *Cloud Computing*

Si bien en el mercado existen diversas alternativas de proveedores de soluciones de *Cloud Computing* con prestaciones similares a las mencionadas en el módulo teórico, por políticas de la empresa sólo pueden ser utilizadas aquellas soluciones que han sido homologadas por la casa matriz, en este caso la solución provista por IBM. Igualmente se realizará la comparación con otra herramienta existente en el mercado en base a los informes *Magic Quadrant* de Gartner y se detallarán las ventajas y desventajas de cada una (Gartner, 2016).

Ilustración 9 ***Garnert Magic Quadrant***

Fuente: (Gartner, 2016)

	Ventajas	Desventajas
***SoftLayer* - IBM**	Tiene un historial de larga trayectoria como proveedor de hosting dedicado y ofrece la más amplia gama de configuraciones de servidor en la nube. Es una marca fuerte y tiene relaciones con clientes en todo el mundo, y su base de clientes de *outsourcing* ayudará a impulsar un negocio de centro de datos en la nube.	Aparte de una introducción a principios de 2015 de nuevas opciones de almacenamiento, el conjunto de funciones de *SoftLayer* no ha mejorado significativamente desde la adquisición de IBM a mediados de 2013. *SoftLayer* utiliza su propia tecnología y API, que tiene soporte limitado de herramientas de terceros.
Microsoft Azure	Abarca componentes IaaS (Infraestructura como servicio) y PaaS (Productos como servicios) integrados que funcionan y se sienten como un todo unificado. Microsoft tiene una visión de servicios de infraestructura y plataforma que no sólo son líderes en soluciones independientes, sino que también amplían e interoperan sin problemas con la infraestructura de Microsoft local (basada en *Hyper*-V, Windows Server, *Active Directory* y *System Center*), herramientas de desarrollo (Incluyendo *Visual Studio* y *Team Foundation Server* [TFS]), *middleware* y aplicaciones, así como las ofertas SaaS (Software como servicio) de Microsoft. Microsoft también se está volviendo más abierta y menos dependiente de su franquicia de *Windows*, y el soporte de Azure para Linux y otras tecnologías de código abierto está mejorando rápidamente.	Si bien Microsoft ha cumplido con los plazos prometidos para la introducción de características críticas que ayudan a Azure a satisfacer las necesidades empresariales de seguridad, disponibilidad, rendimiento, flexibilidad de red y administración de usuarios, no todas estas funciones se implementan con el nivel de completitud, facilidad de uso o habilitación API. Es deseada por los clientes empresariales. Estas dificultades se ven agravadas por una documentación desorganizada, incompleta y a veces anticuada, así como por una organización de apoyo que no siempre es capaz de resolver desafíos de implementación complejos, un número limitado de expertos de Azure fuera de Microsoft (consultores o empleados potenciales) y pocas opciones para el entrenamiento de Azure.

Diseño Metodológico

La metodología de todo este proyecto se encuadra dentro de un ciclo de mejora continua PDCA (del inglés *plan-do-check-act*, esto es, planificar-hacer-verificar-actuar). De esta manera, se puede asignar recursos (tiempo, dinero, personas, entre otros), gestionarlos y optimizarlos. Asimismo, permite terminado el ciclo, revisar el proceso y optimizarlo nuevamente a través del ciclo de mejora.

Para llevar adelante el análisis de riesgos me voy a basar en las directrices y recomendaciones propuestas por la norma de Gestión de Riesgos de Seguridad de la información: ISO/IEC 27005:2011. Esta norma fue desarrollada para ayudar en la aplicación de la seguridad de la información bajo un encuadre de gestión de riesgos. Mientras que para la selección y definición de los controles a implementar utilizaré la norma: Código de prácticas para la gestión de la seguridad de la información: ISO/IEC 27002:2013 y la guía de buenas prácticas COBIT (Objetivos de Control para Información y Tecnologías Relacionadas) de ISACA.

Ilustración 10 PDCA

Fuente: (Propia)

Recolección de datos

- Análisis de Información.
- Entrevistas.
- Plantilla Excel 2016 para análisis de riesgos basado en ISO/IEC 27005.

Planificación del proyecto

- *Microsoft Project* 2010.

Diagramas de Procesos

- Visio 2013.
- Bizagi.

Entorno *Cloud*

- Windows 2012 Server.
- MS-SQL Server 2008.
- *Internet Information Server*.
- ASP.NET

Controles

- *QualysGuard Vulnerability Management*.
- HP ArcSight.
- *Password Manager* Pro.
- OpManager.

Relevamiento

Relevamiento Estructural

Las oficinas de Kantar IBOPE Media se encuentran ubicadas en la calle Suipacha 664 pisos 6 y 7 oficinas de la Ciudad Autónoma de Buenos Aires. Cuenta con una planta de aproximadamente 300 empleados en la Ciudad Autónoma de Buenos Aires. Además, posee oficinas técnicas en Rosario, Córdoba y Mendoza.

Dentro de las oficinas de la Ciudad Autónoma de Buenos Aires, se encuentra instalado el *datacenter* principal que alberga la granja de servidores y el centro de conexionado principal de la red de datos.

En los servidores físicos se encuentra instalado un *cluster* de VMware ESXI 6.0 para contar con alta disponibilidad. Un *cluster* es un conjunto de servidores que son vistos como un todo. Mediante esta tecnología se logra que múltiples servidores físicos sean vistos por el sistema de virtualización como un único y gran repositorio de recursos (procesadores, memoria, disco, placas de red), en inglés se suele utilizar la palabra *pool* de recursos. De esta manera, no sólo se puede optimizar el uso de los mismos sino también que ante la falla de alguno de ellos, el sistema de virtualización logre que las máquinas virtuales sigan operando mediante el ajuste y reorganización de dichos recursos.

A nivel de sistemas operativos se utilizan Windows Server 2008/2012 en su versión estándar y como motores de base de datos MS-SQL 2003/2005/2008. La mayoría de las aplicaciones se encuentran desarrolladas en C#.NET, VB.NET, ASP.NET y corren sobre servidores web IIS (*Internet Information Server*) exceptuando algunos desarrollos muy antiguos que aún permanecen en *Visual Basic* y FOX.

Adicionalmente se cuenta con un contrato por servicios de alojamientos en otros dos centros de cómputos externos (IPlan y SkyOnline) para servicios secundarios.

Gran parte de los desarrollos fueron realizados en forma interna por el área de IT. En los últimos 10 años los *softwares* destinados a clientes externos fueron migrando de versiones de escritorio instalables a versiones *web* lo que redujo costos de mantenimiento y soporte; como contrapartida la infraestructura de servidores y el *datacenter* han crecido para poder soportar esta arquitectura.

Como se menciona en párrafos anteriores, en 2016 la empresa inicia un proceso de reingeniería de toda su infraestructura con la finalidad de consolidar sus múltiples centros de

cómputos y toma la decisión migrar hacia un servicio de *cloud computing*, específicamente los servicios de la empresa *SoftLayer* recientemente adquirida por IBM.

Principales Softwares de Clientes Externos

- TCNET: es un *software* que permite analizar la audiencia de TV en tiempo real minuto a minuto haciendo disponible, datos de audiencia, imágenes y gráficos que permiten un rápido análisis de la competencia y la toma de decisiones, especialmente en los programas que se transmiten "en vivo".
- ADMEDIA: es una aplicación que permite realizar exhaustivos controles publicitarios y análisis de competencia en todos los multimedios. Cuenta con dos grandes módulos dentro de la misma herramienta que permiten hacer el análisis mensual de la inversión publicitaria en multimedios y permite hacer el control publicitario diario en multimedios.
- TVDATA: es un *software* amigable que permite realizar un sinfín de consultas que van desde simples informes de ranking por canales, programas o bloques horarios, pasando por la creación de pautas de pre y post evaluación de campañas publicitarias, para llegar al análisis de perfiles de programa, etc.
- AD ALERT: es una aplicación web que permite hacer un seguimiento de nuevos avisos comerciales, visualización de las creatividades vía *streaming* y análisis multimedios (TV Abierta, TV Paga, Radio, Periódicos, Revistas)
- MEDIA WORKSTATION: es un programa que permite analizar en profundidad los datos de audiencia de televisión ya que posibilita la realización de una gran variedad de análisis y que revoluciona la manera de entender la información asociada a audiencias, añadiendo a los tradicionales indicadores *rating*, alcance y frecuencia otros indicadores innovadores como duplicación de audiencias, alcance exclusivo, asiduidad, origen y destino, análisis de espectadores grandes, medianos y pequeños, fidelidad, consumos exclusivos, etcétera.

- E-RADIO: es una aplicación que permite realizar variados análisis sobre el mercado radial. Entre sus principales funcionalidades este *software* permite visualizar ranking de emisoras, curvas de audiencia, perfil de emisoras, curvas de tendencia y evolución.
- PORTAL E-MONITOR: es una herramienta web que ofrece la unificación de la información analítica de las altas comerciales y de su creatividad.
- OMR (*Outdoor Media Ratings*): el propósito de este sistema es proveer los índices de circulación frente a soportes publicitarios, o un conjunto de ellos, ubicados en el área de medición, detallados por nivel socio económico, sexo y grupos de edades.
- CHOICES 4: es una herramienta que permite explotar los datos de estudios sobre personas, estilos de vida, consumo de medios y de productos.

Pantalla principal de TC.Net para la publicación del rating de televisión en tiempo real:

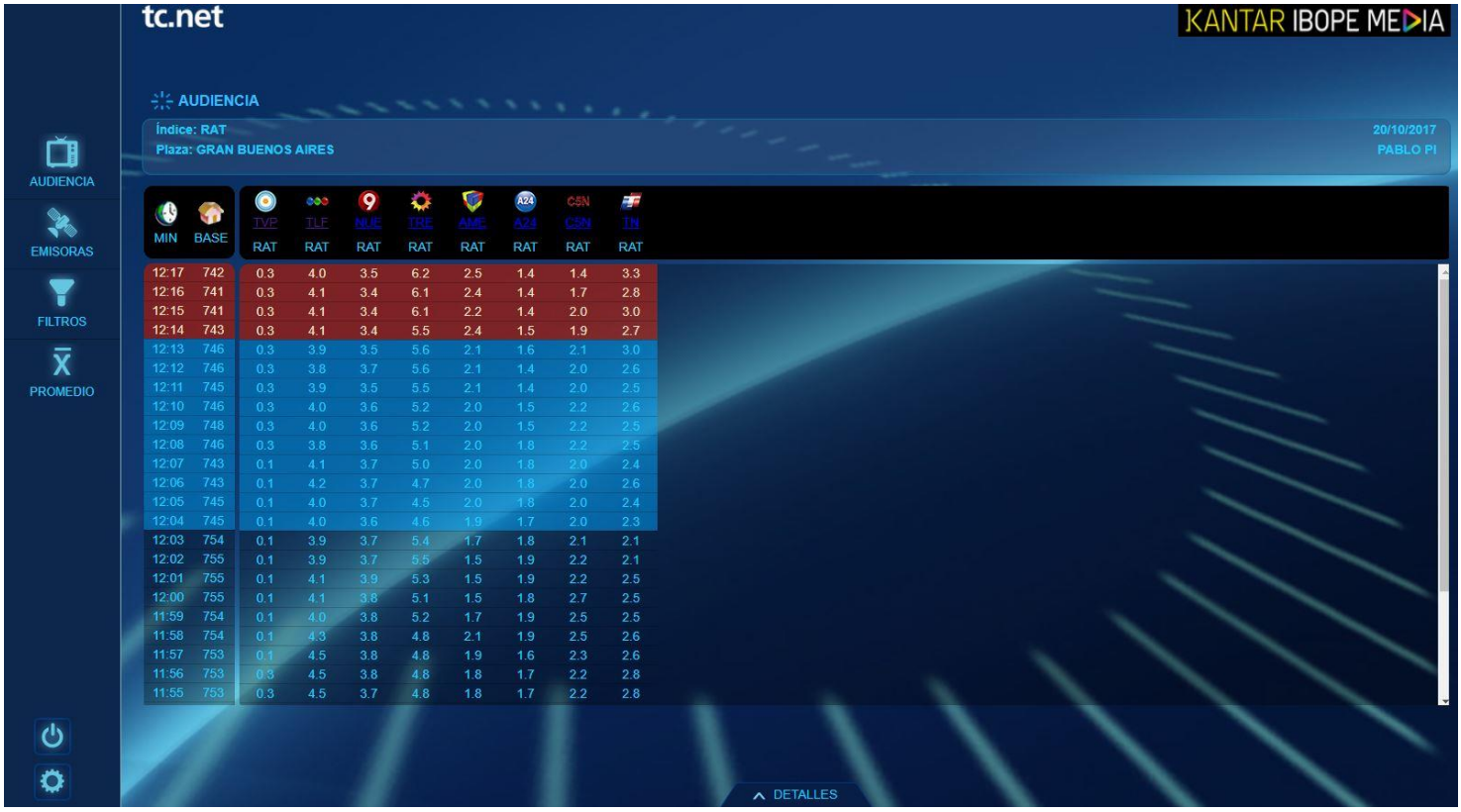


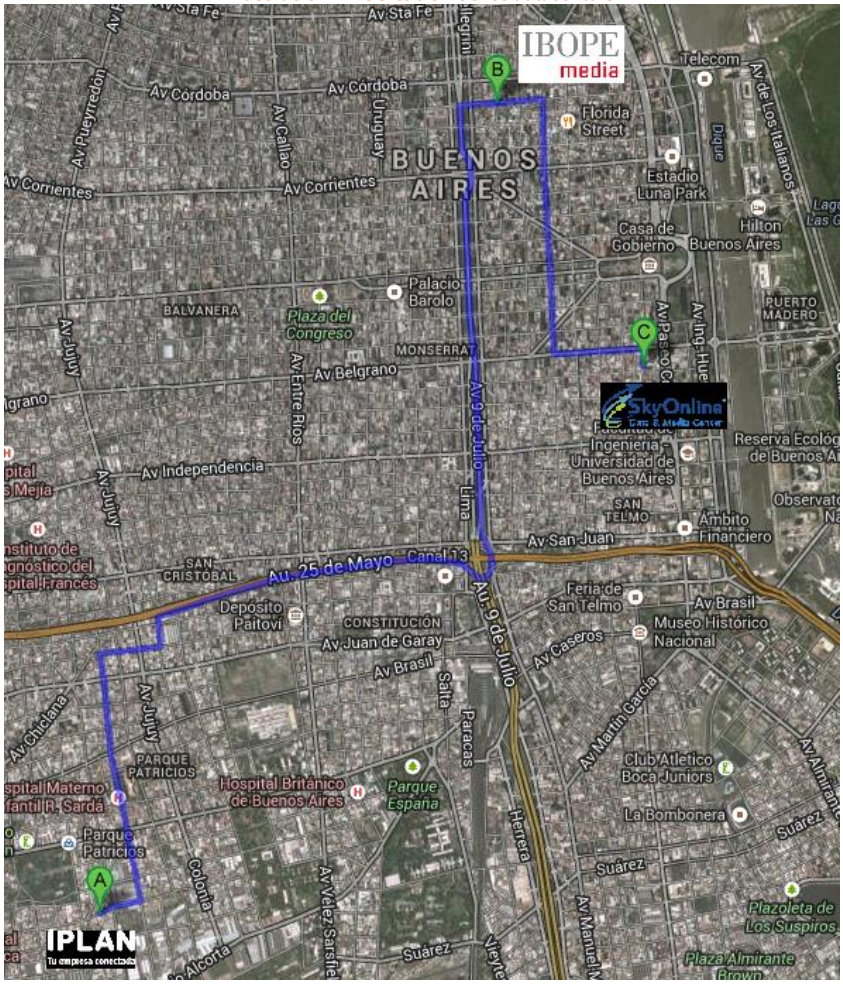
Ilustración 11 TC.Net

Fuente: (Propia)

Ubicación física de los *Datacenters*

Como fue mencionado en el punto anterior la empresa cuenta con tres centros de cómputos: uno ubicado dentro de sus oficinas principales y los otros dos dentro de las instalaciones de proveedores de servicios de alojamiento. Esta estructura fue diseñada para lograr la alta disponibilidad, principalmente para los servicios de medición de audiencia.

Ilustración 12 Ubicación de los *datacenters*



A **Kantar IBOPE Media** - Suipacha 664 piso 6, San Nicolas,CABA.

B **IPLAN** - Los Patos 2948, Parque Patricios, CABA.

C **SkyOnline** – Balcarce 479, Monserat, CABA.

Fuente: (Propia)

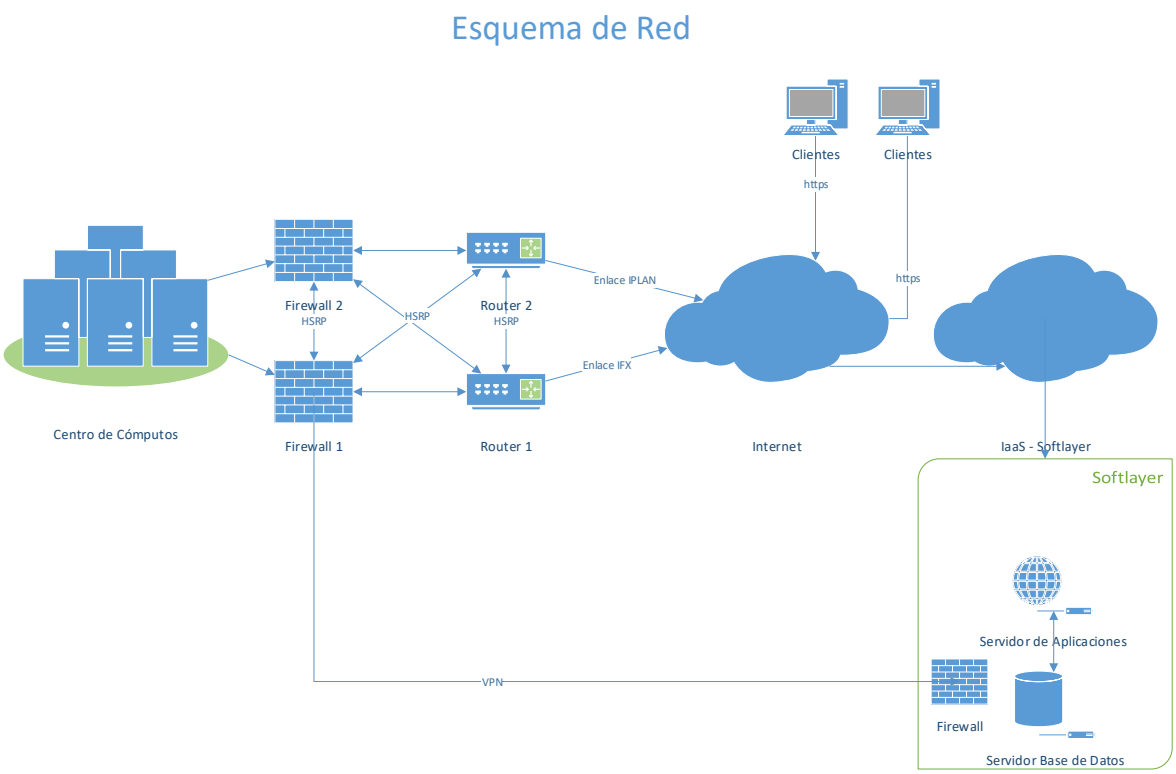
Esquema de Red

La red de la empresa está basada en una topología física de “estrella”. La mayor parte del cableado se concentra en el centro de cómputos, donde se encuentran los dispositivos principales de comunicaciones, enlaces de Internet y los troncales hacia los sitios remotos.

El cableado horizontal de la red está materializado por tendidos UTP categoría 6A, operando a una velocidad de transmisión de 100/1000 Mbps dependiendo del adaptador de red de las estaciones de trabajo (100/1000 Mbps) o servidores (1000 Mbps) y la velocidad de los puertos de los *switches* donde se conectan. El cableado vertical o *backbone* se encuentra materializado principalmente por tendidos de fibra óptica multimodo. A nivel lógico, la red se encuentra montada sobre protocolo TCP/IP y segmentada en VLANs (red de área local virtual). La utilización de VLANs mejora considerablemente la seguridad y la performance de la red. El acceso a internet cuenta con una configuración de alta disponibilidad mediante el uso de equipos de red redundantes.

La interconexión de la red local de Kantar IBOPE Media con el servicio en la nube estará hecha mediante una conexión VPN (*Virtual Private Network* o Red Privada Virtual). De esta manera se garantiza que el tráfico entre ambos sitios se encuentre cifrado de manera que no pueda ser fácilmente interceptado.

Ilustración 13 Esquema de Red



Fuente: (Propia)

Relevamiento Funcional

Organigrama

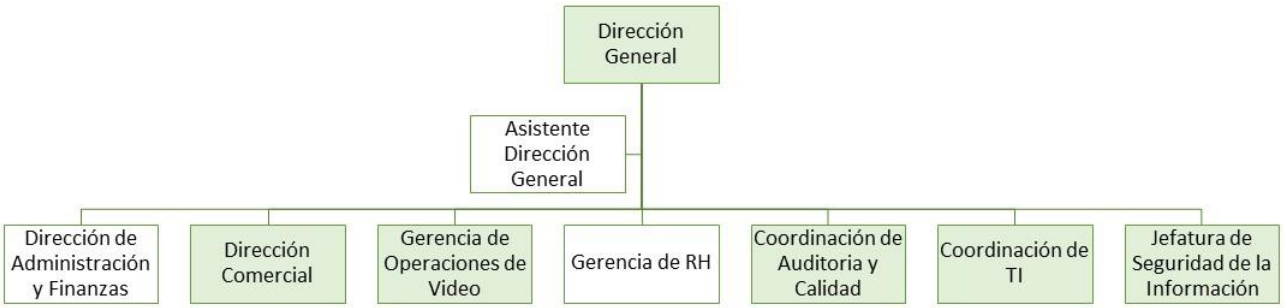


Ilustración 14 Organigrama

Fuente: (Propia)

Funciones de las Áreas

Dirección General: tiene como finalidad implementar los objetivos a mediano y largo plazo definidos por el CEO de la empresa y los accionistas.

Dirección de Administración y Finanzas: su misión es llevar adelante toda la gestión administrativa y contable de la empresa.

Dirección Comercial: su función principal es ser la fuerza de venta de los productos y el principal contacto con los clientes.

Gerencia de Operaciones de Video: su tarea consiste en realizar todos los procesos necesarios para producir los datos de rating de televisión y radio.

Gerencia de RH: su objetivo es la gestión integral de los recursos humanos de la empresa.

Coordinación de Auditoría y Calidad: su principal actividad es la de auditar y controlar los diferentes procesos de la empresa.

Coordinación de TI: tiene a su cargo la tarea de implementar y mantener la infraestructura tecnológica que da soporte a la operación.

Jefatura de Seguridad de la Información: liderar el sistema de gestión de seguridad de la información con el objetivo de proteger debidamente los activos de la información de la empresa.

Partes Interesadas Claves

Las siguientes personas o grupos constituyen las principales partes interesadas del presente proyecto y por tanto es necesario su involucramiento y conocimiento para el éxito del mismo.

Dirección General: desde su posición es el responsable principal de que las directivas de la casa matriz se concreten. En este caso, un cambio en la estrategia tecnológica.

Coordinación de Auditoría y Calidad: debido a que lleva adelante la relación con los organismos externos de control debe asegurarse que los cambios no afecten al cumplimiento de las normas y políticas vigentes.

Coordinación de TI: una de las principales áreas involucradas porque la nueva directiva tiene impacto en el desarrollo de nuevas soluciones de *softwares*.

Gerencia de Operaciones de Video: debe estar en conocimiento porque seguramente en el mediano plazo sus procesos de producción de información se vean afectados por los cambios producidos en los *softwares* de clientes.

Procesos de negocios

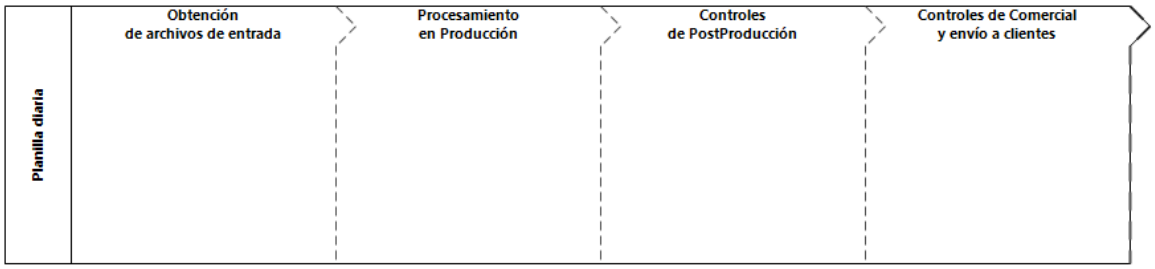
El proceso de negocio actual consta de 4 fases: Obtención de archivos de entrada, Procesamiento, Controles de Post-Producción y Controles del área Comercial y envío a clientes.

- Obtención de los archivos de entrada: dichos archivos se descargan de servidores SFTP ubicados en la casa matriz en Brasil.
- Procesamiento en Producción: los archivos previamente descargados alimentan con sus datos a los *softwares* de producción. El resultado obtenido serán los archivos que alimentan de datos a los *softwares* de clientes.
- Controles de Post-Producción: una vez finalizado el proceso se realizan controles de consistencia de datos, comparativas con tendencias y datos históricos.
- Controles del área Comercial y envío a clientes: el área Comercial realiza los últimos controles de calidad y libera los datos a los clientes.

Este proceso es soportado por una infraestructura de servidores propios, la cual ya fue descripta en el apartado de Relevamiento Estructural.

Publicación de datos a clientes - Fases

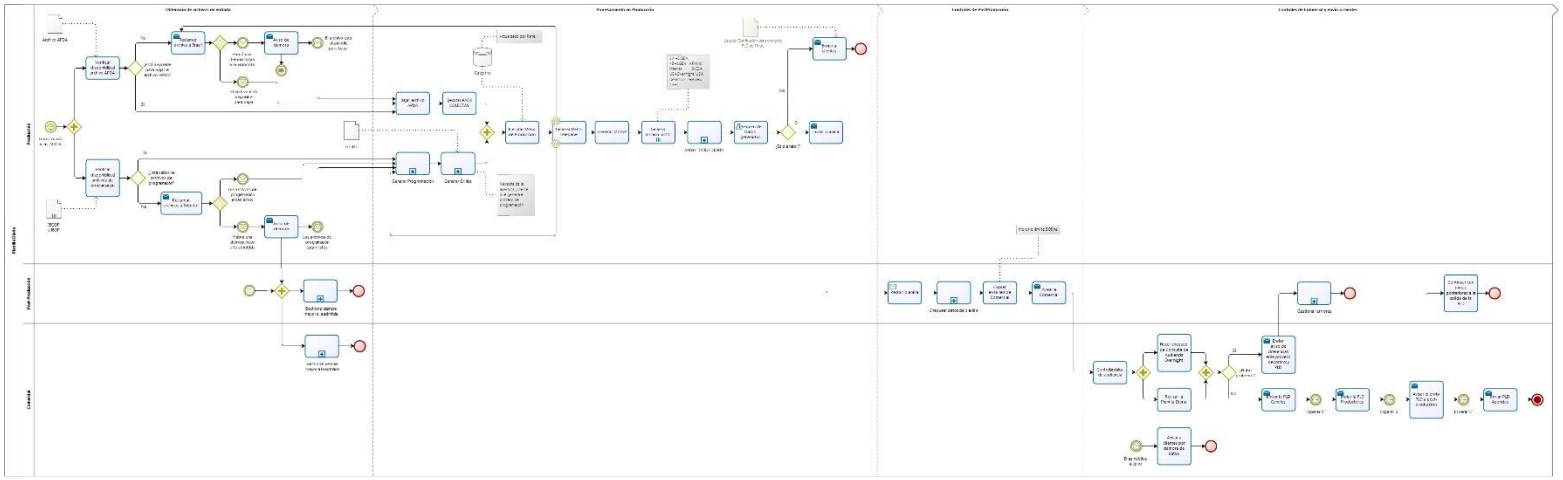
Ilustración 15 Planilla Diaria Fases



Fuente: (Propia)

Publicación de datos a clientes - Diagrama

Ilustración 16 Diagrama BPNM



Fuente: (Propia)

Diagnóstico

La empresa cuenta con un sistema de gestión de seguridad de la información implementado en 2007. El mismo se encuentra basado en la norma Sistema de Gestión de Seguridad de la Información: ISO/IEC 27001:2013 y por lo tanto cuenta con una estructura de controles de seguridad implementados totalmente en el marco de lo exigido por la norma Código de prácticas para la gestión de la seguridad de la información: ISO/IEC 27002:2013.

La norma está dividida en 14 dominios, cuenta con 35 objetivos de control y define 114 controles que deben ser implementados. Estos controles fueron diseñados para una infraestructura física estándar, es decir, que cuenta con una serie de servidores físicos cada uno con su sistema operativo, aplicaciones y motores de bases de datos respectivos.

Si realizamos un breve repaso de alguno de los controles, podemos darnos cuenta fácilmente como dejan de ser efectivos o inaplicables cuando pasamos del centro de cómputos propio a la nube. Por ejemplo, podemos citar el caso de los controles de seguridad física del centro de cómputos, como ser el control de factores ambientales (temperatura y humedad), detectores de humo, sistemas contra incendios o mantenimiento del grupo electrógeno que dejan de ser practicables por las características propias de un entorno *cloud*, ya que es posible que como cliente no tengamos siquiera certezas de donde están residiendo los datos físicamente, tranquilamente pueden estar en uno o varios países extranjeros. Esto último incide también en los controles de seguridad lógica destinados a dar cumplimiento a la legislación argentina de protección de datos personales (Ley 25.326: Protección de los Datos Personales, 2000), dado que dependiendo en qué país estén los datos, es posible que haya leyes que se contrapongan a la legislación argentina, como ya fue mencionado anteriormente en el marco teórico. Otro ejemplo lo encontramos en los controles que se realizan sobre la actividad de los administradores: estos también se verán afectados con el cambio porque dentro del entorno *cloud* la capa que da soporte al servicio *cloud* es administrada por empleados del proveedor de servicio quienes podrían acceder a los datos de la empresa.

Como se indicó en el párrafo introductorio, como parte de su estrategia tecnológica la empresa decide adoptar el *cloud computing* para migrar su infraestructura tecnológica como forma de ir disminuyendo la cantidad y tamaño de *datacenters* contratados que en la actualidad posee.

El problema actual, como se mencionó en el primer párrafo de esta sección, consiste en que no es posible transferir los controles de seguridad de la información vigentes propios de una infraestructura física de manera transparente al nuevo ambiente virtual; ya que el mismo presenta nuevos riesgos que aún no habían sido identificados y evaluados apropiadamente, hasta que comencé a realizar el presente trabajo final de graduación. La carencia o inexistencia de un análisis de las posibles amenazas, impactos y riesgos relacionados a esta transferencia conduciría a la posibilidad de exponer a la empresa a un ataque informático en las aplicaciones montadas en esta nueva plataforma.

El análisis de amenazas y riesgos incluido en el presente trabajo, junto con la definición de los controles de seguridad necesarios que deben implementarse, mitigarán el impacto en el nuevo entorno de manera de asegurar adecuadamente los activos de información de la empresa.

Propuesta de solución general

Tomando como base los requerimientos normativos que la empresa debe cumplir para el desarrollo de sus actividades y para mantener su homologación como empresa medidora de audiencia de televisión y radio, se realizará un análisis de riesgos guiado por la norma ISO/IEC 27005:2011 para poder evaluar las amenazas a la que estarían expuestos los activos de la información que se montarán sobre la nube, de manera de definir los controles a implementar dentro del entorno de *cloud computing* basados en la norma ISO/IEC 27002:2013 y COBIT para mantener un programa de seguridad de la información efectivo.

Diagrama del Proceso de Gestión de Riesgo de Seguridad de la Información

Todo el análisis se realizará dentro del marco de proceso de gestión de riegos de seguridad de la información.

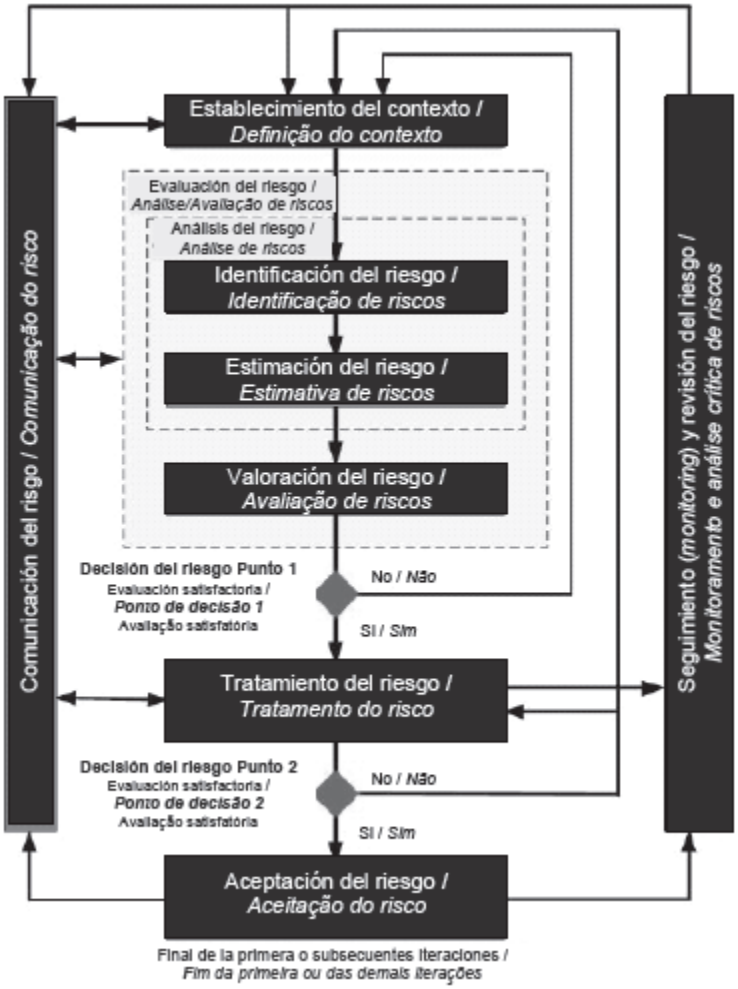


Ilustración 17 Proceso de Gestión de Riesgos

Fuente: (IRAM - Norma ISO/IEC 27005)

La norma Gestión de Riesgos de Seguridad de la información: ISO/IEC 27005:2011 es un estándar internacionalmente aceptado para la administración de riesgos de seguridad de la información. Forma parte de la serie de estándares internacionales de seguridad ISO 27000 desarrollados por la Organización Internacional para la Estandarización (ISO) y la Comisión

Electrotécnica Internacional (IEC) y publicados en nuestro país por el Instituto Argentino de Normalización y Certificación (IRAM). La serie 27000 contiene las mejores prácticas en seguridad de la información para desarrollar, implementar y mantener un sistema de gestión de la seguridad de la información.

En el caso específico de la ISO/IEC 27005:2011 esta norma se ocupa de la gestión de riesgos en seguridad de la información brindando recomendaciones y lineamientos para la evaluación de riesgos de seguridad en la Información. El proceso de análisis propuesto por la norma atraviesa las siguientes fases:

- Establecimiento del contexto
- Evaluación del riesgo
- Tratamiento del riesgo
- Aceptación del riesgo
- Comunicación del riesgo
- Monitorización y revisión del riesgo

Requerimientos funcionales y no funcionales

Listado de requerimientos funcionales

Para una correcta evaluación, la matriz deberá poder:

- Identificar los activos de información y su clasificación
- Identificar sistemas operativos
- Identificar los motores de base de datos
- Identificar los lenguajes de programación y *frameworks* utilizados por la aplicación
- Identificar los procesos de intercambio de información (hacia los clientes)
- Identificar las posibles amenazas
- Contemplar todas las etapas del ciclo de vida de la aplicación
- Diagrama con el perfil de riesgos
- Listado general riesgos
- Listado de mitigaciones
- Listado de controles

- Listado de riesgos aceptados
- Reporte final de la evaluación

Listado de requerimientos no funcionales

Usabilidad

- Deberá contar con una interfaz de usuario sencilla.
- Deberá permitir una carga auto guiada de los datos
- Deberá tener un buen tiempo de respuesta

Restricciones de la tecnología a utilizar

- Deberá estar desarrollado con productos de ofimática Microsoft versión 2016 dado que son los únicos homologados por la empresa.
- Sólo se podrán utilizar los sistemas operativos y motores de base de datos homologados por la casa matriz que se detallan a continuación:
    - Windows 7
    - Windows 8.1
    - Windows 2008 Server
    - Windows 2012 Server
    - MS-SQL 2008

Seguridad

- Deberán incorporarse dentro del sistema de copias de respaldo, todos los entregables resultantes de este trabajo.
- Las hojas de cálculo y los reportes deberán estar cifrados y protegidos con contraseñas según lo establecido en las políticas de la empresa para la información confidencial.

Comunicaciones

- Se deberá contar con un acceso a internet por fibra óptica de 10 Mb para las pruebas técnicas contra la plataforma *cloud*.

- El acceso a internet no deberá tener restricciones a nivel del *firewall* para no interferir con el funcionamiento de las herramientas de seguridad empleadas durante las pruebas.

Hardware

- Se necesitará una *notebook* con los siguientes requerimientos para poder ejecutar las tareas de análisis:
    - Espacio en disco: 20 GB
    - Memoria: mínimo 1GB, recomendado 2GB o más
    - CD-DVD
    - Puerto USB

Integridad

- Se deberán contemplar medidas que permitan asegurar la integridad de los datos ingresados y los resultados obtenidos.

Regulatorios

- Deberá contemplar los aspectos legales y normativos que la empresa debe cumplir como parte de su funcionamiento:
    - Política de Seguridad de la Información y IT de WPP.
    - Manual de normas mínimas para la medición de audiencia de TV y Radio de la CCMA (Cámara de Control de Medición de Audiencia),
    - Ley 25.326 de Protección de los Datos Personales
    - *Sarbanes-Oxley*,
    - *European General Data Protection Regulation*,

Desarrollo

En los siguientes módulos se desarrollará el análisis de riesgo, se identificarán los controles, se evaluará el riesgo residual, además se presentará la metodología para el análisis de los costos. Por último, se presentarán los resultados y conclusiones del trabajo realizado.

Cloud Computing Risk Assessment

En esta sección se va detallar la evaluación del riesgo realizada bajo la Norma de Gestión de Riesgos de Seguridad de la información: ISO/IEC 27005:2011. Este es el proceso de identificar, estimar y priorizar los riesgos de seguridad de la información a los que se expondrá la empresa dentro de un entorno de *cloud computing.* Como parte de la evaluación se identificarán las amenazas que pueden afectar a este ambiente, cuáles vulnerabilidades pretenden explotar dichas amenazas; además, se estimará la probabilidad de ocurrencia y se analizará el impacto que tendría en caso de suceder. Con estas variables se podrá determinar el nivel de riesgo. El análisis realizado será de carácter cualitativo basándose en el juicio experto del oficial de seguridad, el coordinador de IT y el ingeniero senior de infraestructura.

Conceptos claves

Antes de avanzar con la evaluación de riesgos es importante tener en claro los siguientes conceptos:

- Riesgo: estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización. (MAGERIT, 2012).
- Amenaza: causa potencial de un incidente que puede causar daños a un sistema de información o a una organización. (ISO 27001:2009).
- Vulnerabilidad: Defecto o debilidad en el diseño, implementación u operación de un sistema que habilita o facilita la materialización de una amenaza. (MAGERIT, 2012)
- Impacto: magnitud del daño causado por el aprovechamiento de una amenaza sobre una vulnerabilidad (ISACA, 2014).
- Probabilidad de Ocurrencia: La probabilidad es una indicación de la probabilidad de que se pueda ejercer una vulnerabilidad potencial dado el entorno de amenaza. (NIST, 2012).
- Nivel de riesgo: es el resultado del cálculo entre la probabilidad de ocurrencia de que una amenaza se concrete y el impacto que esta genere en la empresa (ISACA, 2014).

Escalas

Para el proceso de evaluación del riesgo se utilizarán los parámetros descriptos a continuación en escalas, con el fin de valorizar la probabilidad de ocurrencia, el impacto y el nivel de riesgo. Estos criterios se encuentran definidos por el NIST (Instituto Nacional de

Normas y Tecnología, USA) en su publicación "800-30: *Risk Management Guide for Information Technology Systems*".

Probabilidad de ocurrencia

Probabilidad de ocurrencia	Valor	Definición de probabilidad de la frecuencia de ocurrencia:
Muy Alta	4	es casi seguro que ocurrirán errores, accidentes o actos de la naturaleza.
Alta	3	es muy probable que ocurra un error, accidente o acto de la naturaleza
Moderada	2	es algo probable que ocurra un error, accidente o acto de la naturaleza
Baja	1	no es probable que ocurra un error, accidente o acto de la naturaleza.
Muy Baja	0	Es muy poco probable que ocurra un error, accidente o acto de la naturaleza.

Impacto

Magnitud del Impacto	Valor	Definición de Impacto
Muy Alto	4	Se podría esperar que el evento de amenaza tenga varios efectos adversos severos o catastróficos en las operaciones de la organización, los activos de la organización, los individuos, otras organizaciones o la Nación.
Alto	3	Se podría esperar que el evento de amenaza tenga un efecto adverso grave o catastrófico en las operaciones de la organización, los activos de la organización, los individuos, otras organizaciones o la Nación. Un efecto adverso grave o catastrófico significa que, por ejemplo, el evento de amenaza podría: provocar una degradación o pérdida severa de la capacidad de la misión en una medida y duración que la organización no pueda llevar a cabo una o más de sus funciones primarias ; resultar en un daño importante a los activos de la organización; dar lugar a pérdidas financieras importantes; o resultar en daño severo o catastrófico a individuos que implican pérdida de vidas o lesiones serias que amenazan la vida.
Moderado	2	Se podría esperar que el evento de amenaza tenga un efecto adverso serio en las operaciones de la organización, los activos de la organización, los individuos de otras organizaciones o la Nación. Un efecto adverso serio significa que, por ejemplo, el evento de amenaza podría: provocar una degradación significativa de la capacidad de la misión en la medida y duración en que la organización pueda desempeñar sus funciones primarias, pero la efectividad de las funciones se reduce significativamente ; resultar en un daño significativo a los activos de la organización; dar lugar a pérdidas financieras significativas; o resultar en un daño significativo a las personas que no implica pérdida de vidas o lesiones serias que amenacen la vida.
Bajo	1	Se podría esperar que el evento de amenaza tenga un efecto adverso limitado sobre las operaciones de la organización, los activos de la organización, los individuos de otras organizaciones o la Nación. Un efecto adverso limitado significa que, por ejemplo, el evento de amenaza podría: provocar una degradación en la capacidad de la misión en la medida y duración en que la organización pueda desempeñar sus funciones primarias, pero la efectividad de las funciones se reduce notablemente; resultar en un daño menor a los activos de la organización; dar lugar a pérdidas financieras menores; o resultar en un daño menor a las personas.
Muy Bajo	0	Ningún impacto significativo. Se podría esperar que el evento de amenaza tenga un efecto adverso insignificante sobre las operaciones de la organización, los activos de la organización, los individuos de otras organizaciones o la Nación.

Niveles de Riesgo

	Probabilidad del escenario de incidentes	Muy baja (Muy improbable)	Leve (Improbable)	Media (Posible)	Alta (Probable)	Muy alta (Frecuente)
Impacto Impacto	Muy bajo	0	1	2	3	4
	Leve	1	2	3	4	5
	Medio	2	3	4	5	6
	Alto	3	4	5	6	7
	Muy alto	4	5	6	7	8

Ilustración 18 Estimación de Niveles de Riesgo
Fuente: (IRAM - Norma ISO/IEC 27005)

Análisis de Riesgos

A continuación, se presenta la matriz con los resultados del proceso de análisis de riesgos. Para este análisis se evaluaron los principales riesgos a los que se encuentran expuestas las infraestructuras de *cloud computing*. En la matriz se detalla cada uno de los riesgos identificados junto con su descripción y la valoración que se ha realizado para medir la probabilidad de ocurrencia, el impacto y el nivel de riesgo.

La selección y definición de los riesgos se realizó tomando como punto de partida la lista de riesgos identificados en las siguientes fuentes adaptándolas a las particularidades del contexto y la tecnología de la empresa:

- ENISA en su publicación: Computación en la nube, Beneficios, riesgos y recomendaciones para la seguridad de la información (enisa.europa.eu, 2009).
- OSWAP en su proyecto: *Cloud Top 10 Security Risks* (owasp.org, 2018).
- CSA en su matriz: *Cloud Controls Matrix* (cloudsecurityalliance.org, 2018).
- HIMSS en su documento del *Cloud Security Toolkit: Top 10 Cloud Security Concerns* (himss.org, 2018)
- *Risk Manager Tool* en su base de conocimiento: *Processo - Computacao em Nuvem_ - Infraestrutura de Computacao em Nuvem e Virtual* (modulo.com.br, 2018)

		Probabilidad de Ocurrencia		Impacto		Nivel de Riesgo	
Riesgo	Descripción	Escala	Valor	Escala	Valor	Escala	Valor
Pérdida de Gobierno	La empresa tiene que dejar en manos del proveedor del servicio *cloud* parte de la gestión de sus datos y la seguridad de los mismos. La falta de claridad en la definición de las responsabilidades podría generar riesgos para la empresa.	Muy Alta	4	Muy Alto	4	Alto	8
Falla de Aislamiento	Dado que en un entorno de *cloud computing* los clientes comparten los recursos físicos es posible que una falla o error en los mecanismos de separación implementados por el proveedor pongan en riesgo la seguridad de los datos de la empresa.	Moderada	2	Muy Alto	4	Alto	6
Riesgo de Cumplimiento	Es posible que el proveedor no pueda proporcionar garantías o evidencia de cumplimiento de los requisitos legales o regulatorios y/o puede no permitir la realización de auditorías. Es posible que algunos tipos de servicios *cloud* no sean compatibles con los requisitos regulatorios que debe cumplir la empresa. Por ejemplo los datos de la empresa pueden estar almacenados o transmitirse entre múltiples países o estados en los cuales puede que no se respeten todos los requerimientos legales que la empresa debe cumplir.	Muy Alta	4	Alto	3	Alto	7
Cliente Cautivo	Una vez elegido un proveedor e implementado el servicio de *cloud computing* puede ser difícil y costoso para la empresa cambiar de proveedor. Por ejemplo si no se cuentan con interfaces estándares para la migración.	Baja	1	Moderado	2	Medio	3
Interfaz de Administración Comprometida	La interfaz de administración para los clientes del servicio *cloud* se encuentra expuesta a internet. Un ataque a esta interfaz podría permitir el acceso indebido a grandes volúmenes de información.	Moderada	2	Muy Alto	4	Alto	6
Cuentas Administrativas	Un usuario con privilegios administrativos altos puede acceder a toda la información por lo que una acción por parte de empleados desleales del proveedor o propios puede provocar que se vean comprometidos los activos de información de la empresa.	Moderada	2	Muy Alto	4	Alto	6

		Probabilidad de Ocurrencia		Impacto		Nivel de Riesgo	
Riesgo	Descripción	Escala	Valor	Escala	Valor	Escala	Valor
Borrado inseguro de la información	Es posible que el proceso de borrado de la información de la plataforma *cloud* no sea seguro y que la información pueda ser recuperada posteriormente.	Moderada	2	Muy Alto	4	Alto	6
Transmisión insegura de datos	Debido a que el acceso a los servicios del entorno *cloud* es siempre a través de internet existe el riesgo que los datos que se consuman o se transmitan entre la nube y la empresa o los clientes se vean comprometidos durante su transferencia.	Moderada	2	Alto	3	Medio	5
Exposición a internet	Debido a que por definición el acceso al entorno cloud es a través de internet las aplicaciones que implemente la empresa para sus clientes enfrenta todos los riesgos asociados a este entorno.	Muy Alta	4	Muy Alto	4	Alto	8
Cortes de red	En el caso de que alguno de los servicios hosteados en la nube tenga una arquitectura híbrida (parte en nube privada parte en nube publica) la caída de la conexión a internet en la empresa puede dejar ese servicio inoperable para los clientes.	Baja	1	Muy Alto	4	Medio	5
Desastres naturales	La ocurrencia de un desastre natural que afecte al proveedor *cloud* podría dejar sin servicio a la empresa.	Muy Baja	0	Alto	3	Medio	3
Privacidad de Datos Personales	Es complejo demostrar que el proveedor del servicio *cloud* gestiona el servicio en concordancia con los requisitos de la ley de protección de datos.	Alta	3	Alto	3	Alto	6
Robo de cuentas	Un *hacker* podría obtener cuentas de usuarios mediante *phishing,* ingeniería social u otras técnicas que pueden permitirle obtener acceso a los servicios *cloud.*	Moderada	2	Alto	3	Medio	5
Recursos insuficientes	Falla en la capacidad de los recursos provisionados por parte del proveedor.	Muy Baja	0	Alto	3	Medio	3
Unicidad de cuentas	Falla en la existencia de una relación univoca usuario-persona puede generar problemas en la trazabilidad de las acciones, dificultar la restriccion de accesos, etc.	Moderada	2	Alto	3	Medio	5

Distribución del Riesgo

El gráfico siguiente nos muestra la distribución de los riesgos en relación al impacto y la probabilidad.

Lista de riesgos identificados:

ID	Descripción
1	Pérdida de Gobierno
2	Falla de Aislamiento
3	Riesgo de Cumplimiento
4	Cliente Cautivo
5	Interfaz de Administración Comprometida
6	Cuentas Administrativas
7	Borrado inseguro de la información
8	Transmisión insegura de datos
9	Exposición a internet
10	Cortes de red
11	Desastres naturales
12	Privacidad de Datos Personales
13	Robo de cuentas
14	Recursos insuficientes
15	Unicidad de cuentas

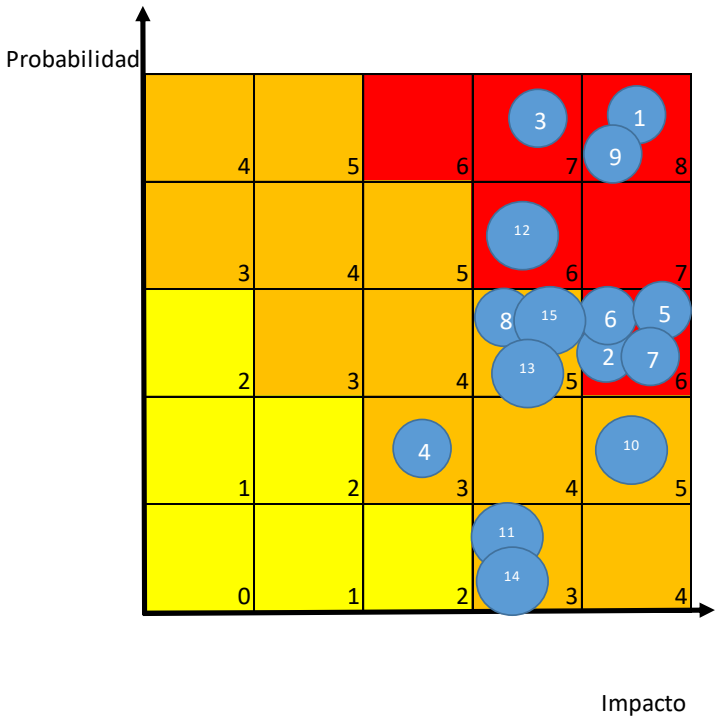


Ilustración 19 Distribución del Riesgo

Fuente: (Propia)

Controles

En esta sección se presentarán las fichas de cada riesgo identificado junto con las descripciones de los controles definidos para mitigar cada uno de los riesgos indicando en cada caso la buena práctica asociada.

Riesgo					
Pérdida de Gobierno					
Descripción					
La empresa tiene que dejar en manos del proveedor del servicio *cloud* parte de la gestión de sus datos y la seguridad de los mismos. La falta de claridad en la definición de las responsabilidades podría generar riesgos para la empresa.					
Probabilidad de Ocurrencia		**Impacto**		**Nivel de Riesgo**	
Escala	**Valor**	**Escala**	**Valor**	**Escala**	**Valor**
Muy Alta	4	Muy Alto	4	Alto	8
Control					
Todo contrato con un proveedor de servicios que acceda a información sensible de la empresa deberá establecer sin ambigüedades las responsabilidades en materia de seguridad y los requisitos a cumplir. Para que esto ocurra se deberá incluir dentro del contrato la adenda de seguridad de la información (*IS Addendum*) desarrollada por las áreas de riesgo corporativo y legales. La misma establece en líneas generales los siguientes requerimientos: revisiones anuales por parte de la empresa sobre el programa de seguridad del proveedor, que el proveedor cuente con políticas de seguridad apropiadas y un programa de seguridad de la información que contemple todos los aspectos necesario para la adecuada protección de los activos de la empresa. (Anexo A)					
Buenas Practicas / Normas Asociadas					
Política de Seguridad de la Información y TI - WPP					
IRAM ISO/IEC 27002:2008 Punto 6 - Organización de la seguridad					
Norma de organización y administración del área de sistemas - CCMA					

Riesgo					
Falla de Aislamiento					
Descripción					
Dado que en un entorno de *cloud computing* los clientes comparten los recursos físicos, es posible que una falla o error en los mecanismos de separación implementados por el proveedor pongan en riesgo la seguridad de los datos de la empresa.					
Probabilidad de Ocurrencia		**Impacto**		**Nivel de Riesgo**	
Escala	**Valor**	**Escala**	**Valor**	**Escala**	**Valor**
Moderada	2	Muy Alto	4	Alto	6
Control					
Para contar con un ambiente seguro el proveedor debe implementar una correcta segregación del entorno (máquinas, redes, hipervisores, etc.), además deberá cifrar las máquinas virtuales y los datos en tránsito, también deberá asegurar la integridad de las máquinas virtuales que ofrece en su *market place y* deberá contar con algún mecanismo de reporte que permita comprobar el aislamiento. Adicionalmente, la empresa deberá implementar su propio esquema de segregación sobre los recursos que le toca administrar como servidores, bases de datos, redes, entre otros de forma que los riesgos queden reducidos. En caso que la información que contengan los equipos implementados en la nube se encuentre clasificada como sensible o confidencial según la escala indicada en la política de clasificación de la información de la empresa se deberá contemplar la implementación de una herramienta adicional para llevar adelante un control más profundo y exhaustivo. Aprovechando que el proveedor de servicio es *Softlayer* de IBM se podrían utilizar las herramientas propias de dicha empresa como *IBM Cloud Secure Virtualization* de forma que la compatibilidad esté asegurada y que la implementación sea más sencilla de realizar. Esta solución permite el asegurar, monitorear y realizar controles de auditoria en tiempo real de las máquinas virtuales.					
Buenas Practicas / Normas Asociadas					
Política de Seguridad de la Información y TI - WPP					
Norma de Clasificación de la Información - KIM					
Norma de seguridad lógica - CCMA					
Norma de organización y administración del área de sistemas - CCMA					
Norma de acceso a la red y transmisión de datos - CCMA					

Riesgo					
Riesgo de Cumplimiento					
Descripción					
Es posible que el proveedor no pueda proporcionar garantías o evidencia de cumplimiento de los requisitos legales o regulatorios y/o puede no permitir la realización de auditorías. Es posible que algunos tipos de servicios *cloud* no sean compatibles con los requisitos regulatorios que debe cumplir la empresa. Por ejemplo los datos de la empresa pueden estar almacenados o transmitirse entre múltiples países o estados en los cuales puede que no se respeten todos los requerimiento legales que la empresa debe cumplir.					
Probabilidad de Ocurrencia		**Impacto**		**Nivel de Riesgo**	
Escala	**Valor**	**Escala**	**Valor**	**Escala**	**Valor**
Muy Alta	4	Alto	3	Alto	7
Control					
Los requisitos de cumplimiento y regulatorios deben ser incluidos en el contrato con el proveedor de servicios. Adicionalmente dicho contrato deberá incluir la adenda de seguridad de la información (*IS Addendum*) desarrollada por las áreas de riesgo corporativo y legales. La misma establece en líneas generales los siguientes requerimientos: revisiones anuales por parte de la empresa sobre el programa de seguridad del proveedor, que el proveedor cuente con políticas de seguridad apropiadas y un programa de seguridad de la información que contemple todos los aspectos necesario para la adecuada protección de los activos de la empresa. (Anexo A).Podemos mencionar en forma adicional que el proveedor de servicio (IBM) posee un portal para que las empresas clientes puedan solicitar reportes de cumplimiento sobre diferentes normativas (SOX, ISO 27000, PCI, HIPAA, Data Privacy) (https://www.ibm.com/cloud-computing/bluemix/es/trust-security-privacy).					
Buenas Practicas / Normas Asociadas					
Política de Seguridad de la Información y TI - WPP					
IRAM ISO/IEC 27002:2008 Punto 15 - Cumplimiento					
COBIT - APO09 Manage service agreements					

Riesgo					
Cliente Cautivo					
Descripción					
Una vez elegido un proveedor e implementado el servicio de *cloud computing* puede ser difícil y costoso para la empresa cambiar de proveedor. Por ejemplo si no se cuentan con interfaces estándares para la migración.					
Probabilidad de Ocurrencia		**Impacto**		**Nivel de Riesgo**	
Escala	**Valor**	**Escala**	**Valor**	**Escala**	**Valor**
Baja	1	Moderado	2	Medio	3
Control					
Se evaluó el servicio del proveedor elegido (Softlayer de IBM) y el mismo cuenta con interfaces estándares para la migración hacia y desde la nube y entre los proveedores más importantes del mercado. Adicionalmente si fuera necesario existen soluciones de terceros para facilitar las migraciones pero consideramos que no serán necesarias por lo antes mencionado.					
Buenas Practicas / Normas Asociadas					
Política de Seguridad de la Información y TI - WPP					

Riesgo					
Interfaz de Administración Comprometida					
Descripción					
La interfaz de administración para los clientes del servicio *cloud* se encuentra expuesta a internet. Un ataque a esta interfaz podría permitir el acceso indebido grandes volúmenes de información.					
Probabilidad de Ocurrencia		**Impacto**		**Nivel de Riesgo**	
Escala	**Valor**	**Escala**	**Valor**	**Escala**	**Valor**
Moderada	2	Muy Alto	4	Alto	6
Control					
Es necesario restringir el acceso a la interfaz de administración del servicio *cloud* a determinadas direcciones IP´s propiedad de la empresa de modo que se limite la posibilidad de que terceros malintencionados intenten acceder. Además las cuentas de acceso a la interfaz deben contar con contraseñas fuertes que cumplan con las políticas de la empresa. La contraseña del administrador general de la plataforma debe ser resguardada en la herramienta de administración de contraseñas Password Manager Pro.					
Buenas Practicas / Normas Asociadas					
Política de Seguridad de la Información y TI - WPP					
Norma de seguridad lógica - CCMA					
IRAM ISO/IEC 27002:2008 Punto 11 - Control de Acceso					
COBIT - DS5.3 - Identity Management					
COBIT - DS5.4 - User Account Management					
COBIT - DS5.7 - Protection of tecnologhy security					

Riesgo					
Cuentas Administrativas					
Descripción					
Un usuario con privilegios administrativos altos puede acceder a toda la información por lo que una acción por parte de empleados desleales del proveedor o propios puede provocar que se vean comprometidos los activos					
Probabilidad de Ocurrencia		**Impacto**		**Nivel de Riesgo**	
Escala	**Valor**	**Escala**	**Valor**	**Escala**	**Valor**
Moderada	2	Muy Alto	4	Alto	6
Control					
Es necesario como punto de partida que se encuentre firmada la adenda de seguridad para que la empresa este habilitada a auditar al proveedor de manera que pueda asegurarse el cumplimiento de los requisitos de seguridad. Un control adicional a implementar será la recolección y análisis de logs. Para esto será necesario conectar el servicio cloud una solución de SIEM (*Security Información Event Management*). Este tipo de soluciones permite recoger, consolidar y analizar los eventos de seguridad. La empresa cuenta con la solución de HP ArcSight implementada en su plataforma *on premise* , que a su vez es monitoreada 24x7x365 por un SOC (*Security Operations Center)* externo contratado con la empresa brasilera Tempest Security Intelligence. Para incluir el servicio *cloud* será necesario implementar los conectores *cloud* para poder capturar los registros generados por el proveedor. Además los servidores que se implementen en la nube deberán pasar por un proceso de *hardening* y estar debidamente actualizados.					
Buenas Practicas / Normas Asociadas					
Política de Seguridad de la Información y TI - WPP					
IRAM ISO/IEC 27002:2008 Punto 10 - Gestión de la operaciones					
IRAM ISO/IEC 27002:2008 Punto 11 - Control de Acceso					
Norma de seguridad lógica - CCMA					
Norma sobre tratamiento de logs - CCMA					
COBIT - DS5.3 - Identity Management					
COBIT - DS5.4 - User Account Management					

Riesgo					
Borrado inseguro de la información					
Descripción					
Es posible que el proceso de borrado de la información de la plataforma *cloud* no sea seguro y que la información pueda ser recuperada posteriormente.					
Probabilidad de Ocurrencia		**Impacto**		**Nivel de Riesgo**	
Escala	**Valor**	**Escala**	**Valor**	**Escala**	**Valor**
Moderada	2	Muy Alto	4	Alto	6
Control					
Es muy difícil de comprobar el efectivo borrado de la información dado que existen herramientas que permiten recuperar información incluso en medios donde se han realizado formateos de bajo nivel. Además de la exigencia al proveedor por poder comprobar este tema se recomienda que los datos sensibles se encuentren cifrados de manera que por mas que puedan ser recuperados después de un borrado no puedan se legibles. Para esto se debe seguir aplicando la política de clasificación vigente y junto con las medidas de protección descritas de acuerdo a cada nivel de clasificación.					
Buenas Practicas / Normas Asociadas					
Política de Seguridad de la Información y TI - WPP					
Norma de seguridad lógica - CCMA					
IRAM ISO/IEC 27002:2008 Punto 7 - Gestión de los Activos					
IRAM ISO/IEC 27002:2008 Punto 10 - Gestión de Comunicaciones y Operaciones					
IRAM ISO/IEC 27002:2008 Punto 15 - Cumplimiento					
COBIT - DS5.8 - Cryptographic Key Management					

Riesgo					
Transmisión insegura de datos					
Descripción					
Debido a que el acceso a los servicios del entorno *cloud* es siempre a través de internet existe el riesgo que los datos que se consuman o se transmitan entre la nube y la empresa o los clientes se vean comprometidos durante su transferencia.					
Probabilidad de Ocurrencia		**Impacto**		**Nivel de Riesgo**	
Escala	**Valor**	**Escala**	**Valor**	**Escala**	**Valor**
Moderada	2	Alto	3	Medio	5
Control					
En este caso se presentan 2 escenarios, la transmisión nube-empresa y la transmisión nube-cliente. Para el primer caso se deberá implementar un acceso VPN *site-to-site* entre la red de la empresa y el proveedor de servicio de *cloud computing* de manera que todo el tráfico por más que se transmita a través de internet, lo haga utilizando un canal cifrado. En el segundo escenario, se deberán restringir el uso de protocolos a aquellos que sean seguros como ser https, ftps, etc..					
Buenas Practicas / Normas Asociadas					
Política de Seguridad de la Información y TI - WPP					
Norma de acceso a la red y transmisión de datos - CCMA					
IRAM ISO/IEC 27002:2008 Punto 11 - Control de Acceso					
IRAM ISO/IEC 27002:2008 Punto 12 - Desarrollo					
COBIT - DS5.10 - Network Security					

Riesgo					
Exposición a internet					
Descripción					
Debido a que por definición el acceso al entorno *cloud* es a través de internet las aplicaciones que implemente la empresa para sus clientes enfrentan todos los riesgos asociados a este entorno.					
Probabilidad de Ocurrencia		**Impacto**		**Nivel de Riesgo**	
Escala	**Valor**	**Escala**	**Valor**	**Escala**	**Valor**
Muy Alta	4	Muy Alto	4	Alto	8
Control					
Este riesgo no es exclusivo del entorno *cloud* sino de toda aplicación expuesta a internet. La empresa ya cuenta con controles definidos para mitigar este riesgo como lo son la inclusión de los requisitos de seguridad en el ciclo de vida de desarrollo de los sistemas, un proceso de gestión de cambios para la puesta en producción de nuevas versiones en forma controlada y segura, la realización de testeos periódicos de la seguridad de las aplicaciones mediante el uso de la herramienta *Web App Scanning* de QualysGuard, además los servidores expuestos a internet deben pasar por un proceso de hardening en el que se le aplican los *baselines* de seguridad y también en forma periódica se realizan escaneos de vulnerabilidades con QualysGuard. Sólo será necesario actualizar los procedimientos para que todos estos procesos incluyan el entorno *cloud.*					
Buenas Practicas / Normas Asociadas					
Política de Seguridad de la Información y TI - WPP					
Norma Desarrollo y Mantenimiento - CCMA					
Norma Control de Cambios - CCMA					
IRAM ISO/IEC 27002:2008 Punto 10 - Gestión de Comunicaciones y Operaciones					
IRAM ISO/IEC 27002:2008 Punto 11 - Control de Acceso					
IRAM ISO/IEC 27002:2008 Punto 12 - Desarrollo					
COBIT - DS5.7 - Protection of tecnologhy security					

Riesgo					
Cortes de red					
Descripción					
En el caso de que alguno de los servicios hosteados en la nube tenga una arquitectura híbrida (parte en nube privada parte en nube pública), la caída de la conexión a internet en la empresa puede dejar ese servicio inoperable para los clientes.					
Probabilidad de Ocurrencia		**Impacto**		**Nivel de Riesgo**	
Escala	**Valor**	**Escala**	**Valor**	**Escala**	**Valor**
Baja	1	Muy Alto	4	Medio	5
Control					
La empresa ya tiene implementadas las medidas y controles necesarios para contar con un acceso a internet con alta disponibilidad provisto de dispositivos de red y enlaces redundantes. Adicionalmente se realizan pruebas periódicas sobre su funcionamiento efectivo. Se deberán actualizar los procedimientos de pruebas para incorporar los controles sobre los servicios que estén hosteados en la nube.					
Buenas Practicas / Normas Asociadas					
Política de Seguridad de la Información y TI - WPP					
Norma de acceso a la red y transmisión de datos - CCMA					
Norma de Contingencia - CCMA					
IRAM ISO/IEC 27002:2008 Punto 10 - Gestión de Comunicaciones y Operaciones					
IRAM ISO/IEC 27002:2008 Punto 14 - Gestión de la Continuidad del Negocio					
COBIT - DS4.1 - IT Continuity					
COBIT - DS5.7 - Protection of tecnologhy security					
COBIT - DS5.10 - Network Security					

Riesgo					
Desastres naturales					
Descripción					
La ocurrencia de un desastre natural que afecte al proveedor *cloud* podría dejar sin servicio a la empresa.					
Probabilidad de Ocurrencia		**Impacto**		**Nivel de Riesgo**	
Escala	**Valor**	**Escala**	**Valor**	**Escala**	**Valor**
Muy Baja	0	Alto	3	Medio	3
Control					
Se presupone que este riesgo de ocurrir debería casi no afectar a un proveedor de *cloud computing* como lo haría con la propia empresa dado que el proveedor cuenta con múltiples centros de cómputos distribuidos en varias regiones del mundo y sus tecnologías están preparadas para brindar servicios de alta disponibilidad y con calidad de servicio. Sin embargo, es necesario que la empresa se proteja debidamente incluyendo las cláusulas necesarias para que el proveedor se comprometa a cumplir con los niveles de servicio contratados.					
Buenas Practicas / Normas Asociadas					
Política de Seguridad de la Información y TI - WPP					
Norma de Contingencia - CCMA					
IRAM ISO/IEC 27002:2008 Punto 14 - Gestión de la Continuidad del Negocio					
COBIT - DS4.1 - IT Continuity					

Riesgo					
Privacidad de Datos Personales					
Descripción					
Es complejo demostrar que el proveedor del servicio *cloud* gestiona el servicio en concordancia con los requisitos de la ley de protección de datos.					
Probabilidad de Ocurrencia		**Impacto**		**Nivel de Riesgo**	
Escala	**Valor**	**Escala**	**Valor**	**Escala**	**Valor**
Alta	3	Alto	3	Alto	6
Control					
Al igual que en el caso de los riesgos por cumplimiento, los requisitos a cumplir por el proveedor en materia de protección de datos personales se deben incluir en el contrato de servicio. Adicionalmente, dicho contrato deberá incluir la adenda de seguridad de la información (*IS Addendum*) desarrollada por las áreas de riesgo corporativo y legales. La misma establece en líneas generales los siguientes requerimientos: revisiones anuales por parte de la empresa sobre el programa de seguridad del proveedor, que el proveedor cuente con políticas de seguridad apropiadas y un programa de seguridad de la información que contemple todos los aspectos necesario para la adecuada protección de los activos de la empresa. (Anexo A). Podemos mencionar en forma adicional que el proveedor de servicio (IBM) posee un portal para que las empresas clientes puedan solicitar reportes de cumplimiento sobre diferentes normativas (SOX, ISO 27000, PCI, HIPAA, Data Privacy) (https://www.ibm.com/cloud-computing/bluemix/es/trust-security-privacy).					
Buenas Practicas / Normas Asociadas					
Política de Seguridad de la Información y TI - WPP					
IRAM ISO/IEC 27002:2008 Punto 15 - Cumplimiento					
COBIT - APO09 Manage service agreements					
COBIT - APO13 Manage Security					

Riesgo					
Robo de cuentas					
Descripción					
Un *hacker* podría obtener cuentas de usuarios mediante *phishing,* ingeniería social u otras técnicas que pueden permitirle obtener acceso a los servicios *cloud.*					
Probabilidad de Ocurrencia		**Impacto**		**Nivel de Riesgo**	
Escala	**Valor**	**Escala**	**Valor**	**Escala**	**Valor**
Moderada	2	Alto	3	Medio	5
Control					
Este no es un riesgo exclusivo del *cloud computing* sino que es transversal a toda la seguridad informática. La mejor práctica para reducir este tipo de riesgos es contar con un programa de concientización en materia de seguridad de la información maduro y constante en el tiempo. Es habitual dentro del programa anual de concientización de la empresa que se incluya la temática del *phishing.* Para esto se ha contratado este servicio como parte de los penetración *test* y en los dos últimos años se contrato a la empresa brasilera Tempest quienes cuentan con una plataforma llamada "El Pescador" que permite hacer campañas de *phishing* y capacitar a los usuarios que caen en las mismas. De esta forma además la empresa cuenta con una medición sobre la efectividad del programa de concientización.					
Buenas Practicas / Normas Asociadas					
Política de Seguridad de la Información y TI - WPP					
Norma de organización y administración del área de sistemas - CCMA					
IRAM ISO/IEC 27002:2008 Punto 8 - Seguridad de los Recursos Humanos					

Riesgo					
Recursos insuficientes					
Descripción					
Falla en la capacidad de los recursos provisionados por parte del proveedor.					
Probabilidad de Ocurrencia		**Impacto**		**Nivel de Riesgo**	
Escala	**Valor**	**Escala**	**Valor**	**Escala**	**Valor**
Muy Baja	0	Alto	3	Medio	3
Control					
Se deberán incorporar dentro del contrato las especificaciones relacionadas a los niveles de servicios contratados. Adicionalmente, el proveedor deberá entregar reportes periódicos que demuestren el cumplimiento de los niveles de servicio. En forma adicional el área de infraestructura de la empresa deberá monitorear los recursos de los servidores implementados en el servicio *cloud* incorporándolos dentro del sistema de monitoreo del NOC (*Network Operations Center*) de la empresa. Actualmente para esta tarea la empresa tiene implementada la solución de *software* OPMANAGER de la compañía ManageEngine.					
Buenas Practicas / Normas Asociadas					
Política de Seguridad de la Información y TI - WPP					
Norma administración y planificación del CPD - CCMA					
IRAM ISO/IEC 27002:2008 Punto 10 - Gestión de Comunicaciones y Operaciones					
COBIT - APO09 Manage service agreements					

Riesgo					
Unicidad de cuentas					
Descripción					
Falla en la existencia de una relación unívoca usuario-persona puede generar problemas en la trazabilidad de las acciones, dificultar la restricción de accesos, etc.					
Probabilidad de Ocurrencia		**Impacto**		**Nivel de Riesgo**	
Escala	**Valor**	**Escala**	**Valor**	**Escala**	**Valor**
Moderada	2	Alto	3	Medio	5
Control					
Se deberá implementar un servicio de federación de identidades para evitar la multiplicidad de usuarios y permitir una administración controlada y centralizada del ciclo de vida de los usuarios. Actualmente el control de acceso de todas las aplicaciones de la empresa está integrado con *Windows Active Directory 2008* mediante varios recursos de *software.* La plataforma *cloud* de Softlayer permite la integración con *Windows* A*ctive Directory* mediante el uso de un conector. Este conector permite la sincronización automática de los usuarios entre la nube y el *Active Directory*					
Buenas Practicas / Normas Asociadas					
Política de Seguridad de la Información y TI - WPP					
IRAM ISO/IEC 27002:2008 Punto 10 - Gestión de la operaciones					
IRAM ISO/IEC 27002:2008 Punto 11 - Control de Acceso					
Norma de seguridad lógica - CCMA					
Norma sobre tratamiento de logs - CCMA					
COBIT - DS5.3 - Identity Management					
COBIT - DS5.4 - User Account Management					

Matriz de riesgo residual

El riesgo residual, es el riesgo estimado, teniendo en cuenta la aplicación de los controles definidos, alternando la probabilidad y el impacto.

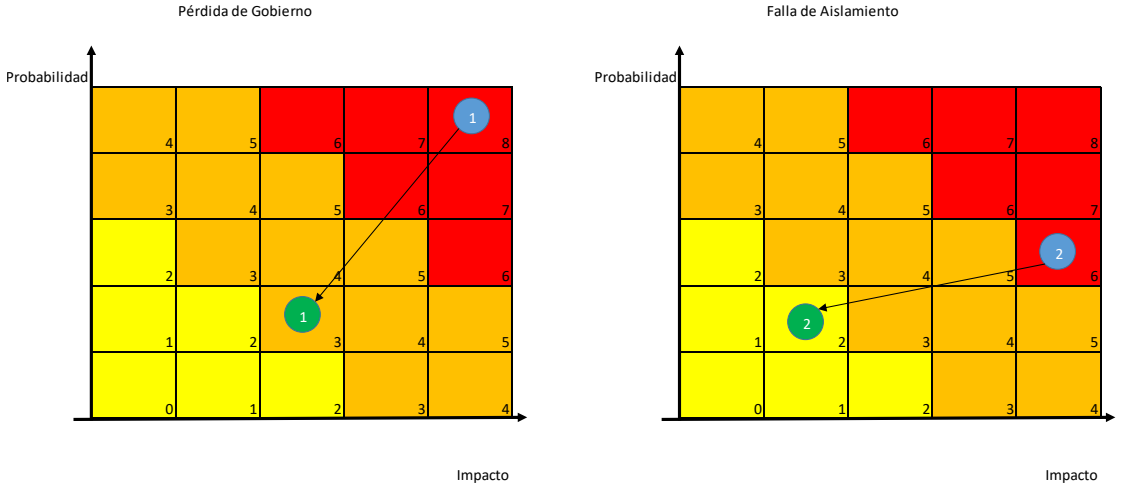
A los fines de este trabajo, he preparado una matriz de riesgo residual para cada uno de los riesgos mencionados anteriormente de manera de graficar la modificación de la probabilidad y el impacto una vez aplicados los controles definidos para cada caso.

		Riesgo Residual					
		Probabilidad de Ocurrencia		Impacto		Nivel de Riesgo	
Riesgo	Descripción	Escala	Valor	Escala	Valor	Escala	Valor
Pérdida de Gobierno	La empresa tiene que dejar en manos del proveedor del servicio *cloud* parte de la gestión de sus datos y la seguridad de los mismos. La falta de claridad en la definición de las responsabilidades podría generar riesgos para la empresa.	Baja	1	Moderado	2	Medio	3
Falla de Aislamiento	Dado que en un entorno de *cloud computing* los clientes comparten los recursos físicos es posible que una falla o error en los mecanismos de separación implementados por el proveedor pongan en riesgo la seguridad de los datos de la empresa.	Baja	1	Bajo	1	Bajo	2
Riesgo de Cumplimiento	Es posible que el proveedor no pueda proporcionar garantías o evidencia de cumplimiento de los requisitos legales o regulatorios y/o puede no permitir la realización de auditorías. Es posible que algunos tipos de servicios *cloud* no sean compatibles con los requisitos regulatorios que debe cumplir la empresa. Por ejemplo los datos de la empresa pueden estar almacenados o transmitirse entre múltiples países o estados en los cuales puede que no se respeten todos los requerimientos legales que la empresa debe cumplir.	Baja	1	Bajo	1	Bajo	2
Cliente Cautivo	Una vez elegido un proveedor e implementado el servicio de *cloud computing* puede ser difícil y costoso para la empresa cambiar de proveedor. Por ejemplo si no se cuentan con interfaces estándares para la migración.	Baja	1	Bajo	1	Bajo	2
Interfaz de Administración Comprometida	La interfaz de administración para los clientes del servicio *cloud* se encuentra expuesta a internet. Un ataque a esta interfaz podría permitir el acceso indebido a grandes volúmenes de información.	Baja	1	Bajo	1	Bajo	2
Cuentas Administrativas	Un usuario con privilegios administrativos altos puede acceder a toda la información por lo que una acción por parte de empleados desleales del proveedor o propios puede provocar que se vean comprometidos los activos de información de la empresa.	Moderada	2	Moderado	2	Medio	4
Borrado inseguro de la información	Es posible que el proceso de borrado de la información de la plataforma *cloud* no sea seguro y que la información pueda ser recuperada posteriormente.	Baja	1	Moderado	2	Medio	3
Transmisión insegura de datos	Debido a que el acceso a los servicios del entorno *cloud* es siempre a través de internet existe el riesgo que los datos que se consuman o se transmitan entre la nube y la empresa o los clientes se vean comprometidos durante su transferencia.	Baja	1	Bajo	1	Bajo	2
Exposición a internet	Debido a que por definición el acceso al entorno cloud es a través de internet las aplicaciones que implemente la empresa para sus clientes enfrenta todos los riesgos asociados a este entorno.	Baja	1	Moderado	2	Medio	3
Cortes de red	En el caso de que alguno de los servicios hosteados en la nube tenga una arquitectura híbrida (parte en nube privada parte en nube publica) la caída de la conexión a internet en la empresa puede dejar ese servicio inoperable para los clientes.	Baja	1	Bajo	1	Bajo	2
Desastres naturales	La ocurrencia de un desastre natural que afecte al proveedor *cloud* podría dejar sin servicio a la empresa.	Muy Baja	0	Bajo	1	Bajo	1
Privacidad de Datos Personales	Es complejo demostrar que el proveedor del servicio *cloud* gestiona el servicio en concordancia con los requisitos de la ley de protección de datos.	Moderada	2	Moderado	2	Medio	4
Robo de cuentas	Un *hacker* podría obtener cuentas de usuarios mediante *phishing,* ingeniería social u otras técnicas que pueden permitirle obtener acceso a los servicios *cloud.*	Baja	1	Moderado	2	Medio	3
Recursos insuficientes	Falla en la capacidad de los recursos provisionados por parte del proveedor.	Muy Baja	0	Bajo	1	Bajo	1
Unicidad de cuentas	Falla en la existencia de una relación univoca usuario-persona puede generar problemas en la trazabilidad de las acciones, dificultar la restriccion de accesos, etc.	Baja	1	Bajo	1	Bajo	2

Mapa de riesgo

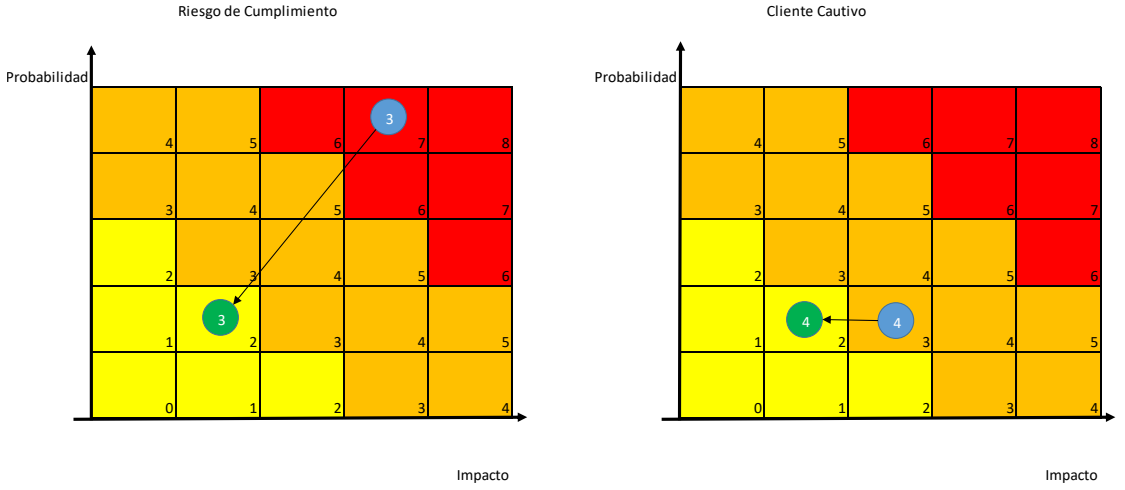
En la siguiente sección vamos a mostrar gráficamente como la aplicación de las mitigaciones propuestas en los controles impacta en el riesgo inherente para obtener el riesgo residual.

Ilustración 20 Mapa de Riesgo 1



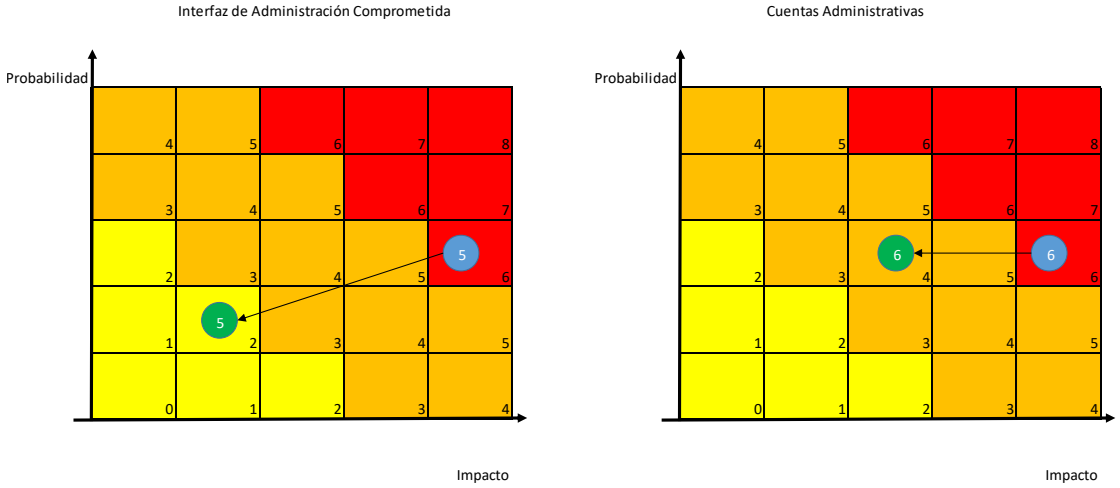
Fuente: (Propia)

Ilustración 21 Mapa de Riesgo 2



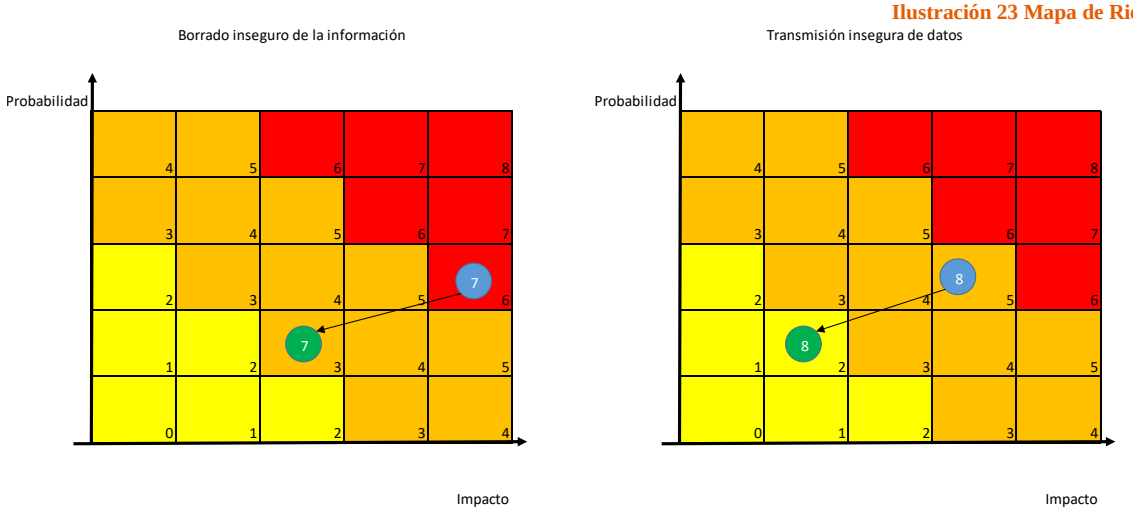
Fuente: (Propia)

Ilustración 22 Mapa de Riesgo 3



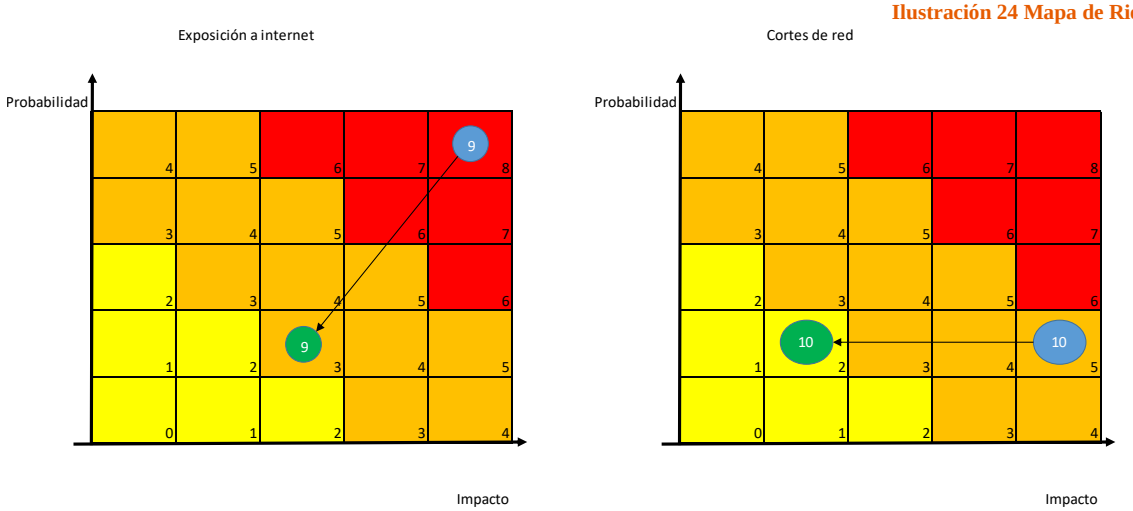
Fuente: (Propia)

Ilustración 23 Mapa de Riesgo 4



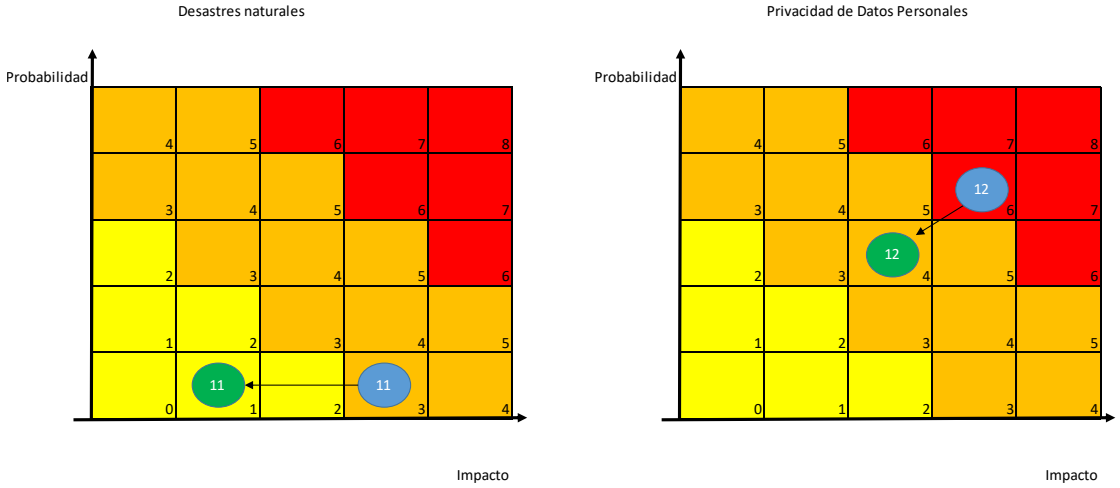
Fuente: (Propia)

Ilustración 24 Mapa de Riesgo 5



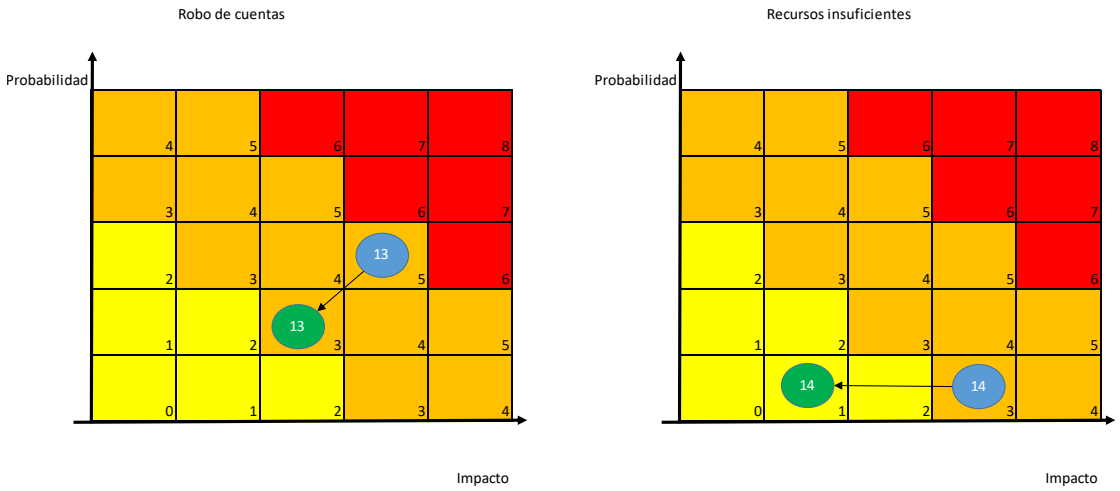
Fuente: (Propia)

Ilustración 25 Mapa de Riesgo 6



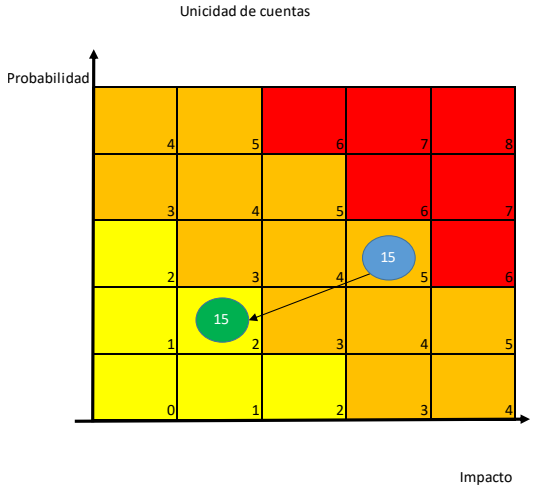
Fuente: (Propia)

Ilustración 26 Mapa de Riesgo 7



Fuente: (Propia)

Ilustración 27 Mapa de Riesgo 8



Fuente: (Propia)

Análisis de Costos

Cuando se habla de seguridad de la información todavía hoy es muy difícil lograr que dentro de las empresas vean en ella algo más que un gasto y muchos proyectos naufragan casi antes de empezar por esta problemática. Una forma aceptada y bastante común para determinar, qué le devuelve a la empresa en términos monetarios una inversión realizada en el marco de un proyecto, es utilizar el cálculo del ROI (*return of investment* o retorno de la inversión).

La fórmula para el cálculo del retorno de la inversión es:

$$ROI = \frac{(Ganacia\ de\ la\ Inversión - Costo\ de\ la\ Inversión)}{Costo\ de\ la\ Inversión} * 100$$

El problema con este cálculo es que para el caso de la seguridad de la información es muy difícil de calcular la ganancia. Por esta razón se ha desarrollado una metodología específica llamada ROSI (*Return On Security Investment* o Retorno de la Inversión en Seguridad) que les permite a las empresas justificar las decisiones financieras relacionadas a los proyectos de seguridad.

El objetivo principal de esta metodología es demostrar que estas inversiones ayudan a prevenir pérdidas. En otros términos, que cuando se invierte en seguridad, lo que se espera es reducir los riesgos que amenazan a los activos. A primera vista parece que no es sencillo cuantificar esta mitigación del riesgo, pero Wes Sonnenreich en su escrito *Return On Security Investment (ROSI): A Practical Quantitative Model* (Sonnenreich, 2005) propone una fórmula sencilla:

$$ROSI = \frac{(Riesgo\ Expuesto * \%\ Riesgo\ Mitigado) - Costo\ de\ la\ Solución}{Costo\ de\ la\ Solución}$$

El riesgo expuesto viene determinado por el total anual de incidentes de seguridad y su impacto económico. Se puede calcular de la siguiente manera:

$$Riesgo\ Expuesto = Costo\ de\ un\ Incidente * Tasa\ de\ Ocurrencia\ Anual$$

A continuación, podemos observar gráficamente como al calcular el ROSI podemos encontrar el nivel óptimo de seguridad al menor costo.

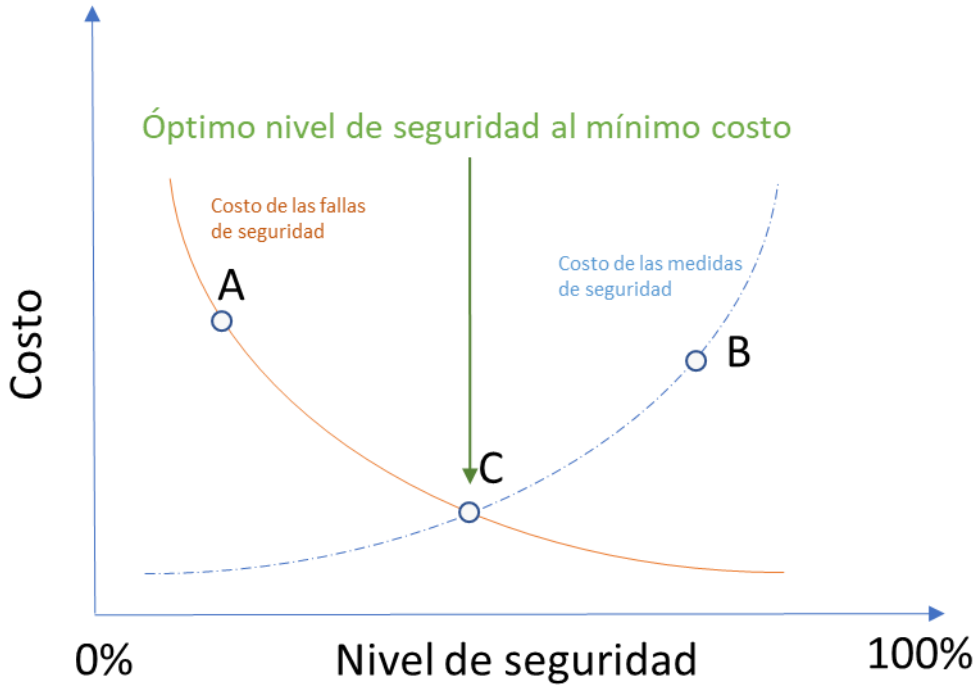


Ilustración 28 ROSI

Fuente: (Propia)

El costo de un incidente puede ser determinado en base a registros históricos de la empresa o bien haciendo una estimación utilizando alguna de las siguientes variables:

- Unidades y procesos de negocios
- Costo de reposición de los activos dañados
- Costo de remediación
- Costo de multas por incumplimiento
- Pérdida de imagen o clientes
- Etc.

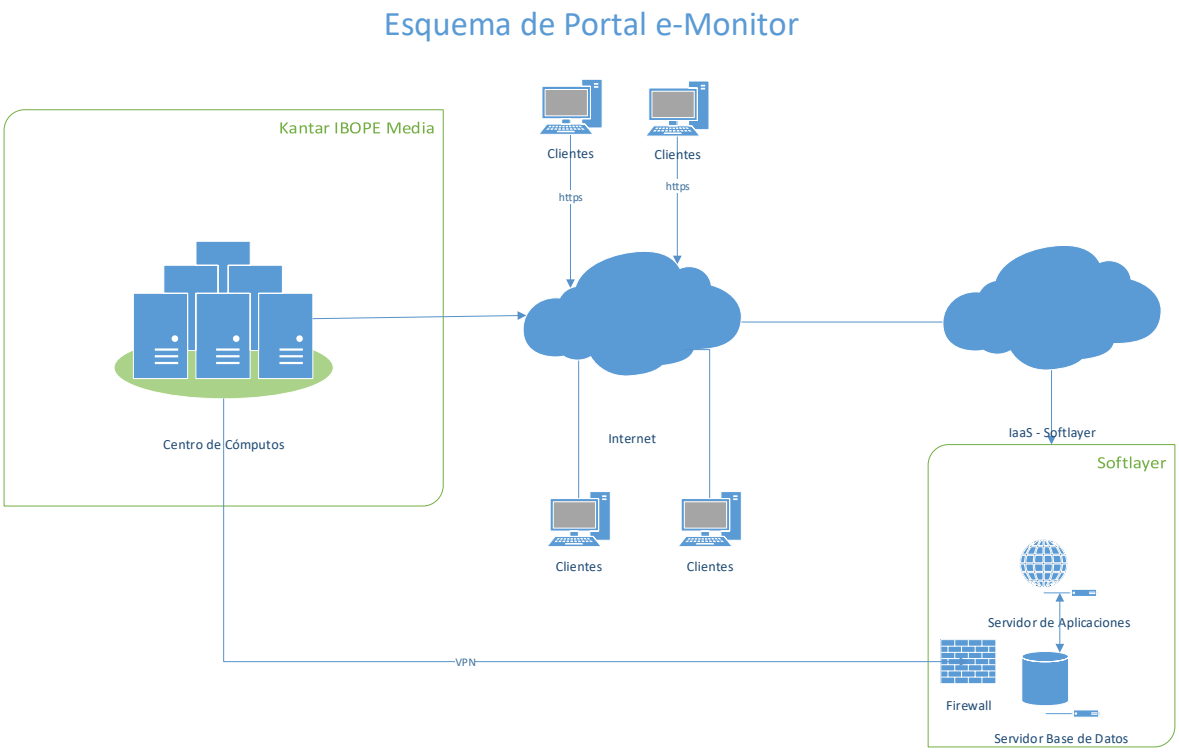
La Tasa de Ocurrencia Anual se puede obtener como ya fue mencionado para el Costo de un Incidente en base a registros históricos o por medio de una estimación.

Un punto importante para lograr un método efectivo para estos cálculos es contar con métricas o registros consistentes.

De esta manera, se puede evaluar la conveniencia de implementar una medida de seguridad en relación al costo de la misma.

Seguidamente, realizaremos el ejercicio de cálculo teórico para la herramienta Portal e-Monitor. Para esto primeramente describiremos brevemente la infraestructura que soporta dicho servicio, la misma está conformada por 2 servidores: uno que ejecuta la aplicación web y otro que contiene la base de datos. Ambos cuentan con un sistema operativo *Windows Server* 2012 y el motor de base de datos es MS-SQL 2008. A continuación, se presenta un diagrama que muestra la implementación descripta.

Ilustración 29 Portal e-Monitor



Fuente: (Propia)

Como quedó definido en la matriz de controles que se obtuvo como resultado del análisis de riesgo, se deberán implementar los siguientes controles:

Riesgo	Control	¿Tiene Costo?	Observaciones
Falla de Aislamiento	Basado en la clasificación de la información de este aplicativo no hace falta implementar la medida propuesta.	N/A	
Interfaz de Administración Comprometida	Implementar VPN e incluir los usuarios en la aplicación para administrar contraseñas *Password Manager* Pro.	NO	Los *softwares* mencionados no requieren de la compra de licencias adicionales.
Cuentas Administrativas	Monitoreo de eventos mediante el SIEM y SOC. Incluir los usuarios en la aplicación para administrar contraseñas *Password Manager* Pro.	SI	
Borrado inseguro de la información	Basado en la clasificación de la información de este aplicativo no hace falta implementar la medida propuesta.	N/A	
Transmisión insegura de datos	Implementar VPN.	NO	No requiere licencias adicionales.
Exposición a internet	Análisis de Vulnerabilidades con QualysGuard. Monitoreo de eventos mediante el SIEM y SOC.	SI	
Cortes de red	Alta disponibilidad de dispositivos de red y enlace redundante	NO	Solución ya existente.
Recursos insuficientes	Monitoreo de infraestructura mediante la aplicación OpManager.	NO	No requiere licencias adicionales.
Unicidad de cuentas	Federación de identidades.	NO	Incluido en el contrato del servicio en la nube.

De los controles enunciados en el cuadro previo, sólo se tendrán en cuenta para el cálculo del ROSI: el análisis de vulnerabilidades con QualysGuard, ~~y~~ el monitoreo de eventos (*logs*) mediante el uso de la herramienta de SIEM (*Security Información Event Management* o Gestión de Eventos e Información de Seguridad) de HP llamada ArcSight y el monitoreo activo por parte del SOC (*Security Operations Center* o Centro de Operaciones de Seguridad) que tiene contratado la empresa. El resto de los controles no presentan un costo adicional para su implementación porque no requieren la compra de licencias adicionales ni equipamiento específico.

Para realizar los cálculos se tomarán los datos del panel de ventas de la empresa (los valores reales fueron modificados por cuestiones de confidencialidad de la información)

MENSUAL 2017					ANUAL 2017	
MONITOR	MULTIM TGI-OTROS	MULTIM AUDIO	VIDEO	TOTAL MENSUAL	MESES	AÑO GROSS
9.044.923	543.302	112.421	12.201.865	21.902.510	12	262.830.117

MONITOR BASICO	Portal e-Monitor	MONITOR VTRACK	MONITOR ADALERT	MONITOR OTROS
4.898.613	3.893.413	25.000	178.422	49.475

Ilustración 30 Panel de Ventas

Fuente: (Propia)

Para el caso puntual de este ejercicio como fue mencionado anteriormente utilizaré el software de clientes Portal e-Monitor.

Siguiendo con lo propuesto para el cálculo del ROSI primero se definen los costos de las variables:

Costo de un incidente por día:	U$S 129780
Tasa de Ocurrencia Anual: (basada en los registros de la herramienta de mesa de ayuda)	5
Riesgo expuesto:	U$S 129780 x 5 = U$S 648900
Costo de la solución:	
1. Control de Vulnerabilidades:	U$S 216 QualysGuard costo anual por el monitoreo de 2 ip´s.
2. Control de eventos (*logs*):	U$S 4794 costo anual incluye licencias de SIEM ArcSight y monitoreo por parte de SOC 7x24 hasta 7GB por día.
TOTAL:	U$S 5010

Ahora se aplica la fórmula del ROSI descripta previamente:

$$ROSI = \frac{(648900 * 0{,}85) - 5010}{5010}$$

El resultado obtenido es:

$$ROSI = 109{,}09\%$$

Como se puede observar en los cálculos anteriores, tomando como base los datos de la herramienta de gestión de incidentes de mesa de ayuda, se ha determinado que la empresa sufre en promedio 5 incidentes anuales sobre el Portal e-Monitor. Basados en la ganancia anual se estimó que la perdida producida por cada incidente ronda los 129780 dólares. El costo de la solución es de 5010 dólares y se proyecta que las mismas bloquearan en 85% de los incidentes. Aplicando el cálculo del ROSI vemos que los resultados arrojados por el mismo~~s~~ demuestran que la solución propuesta justifica la inversión ya que el ahorro

producido a partir de la inversión proporcionaría un reembolso del 109,09% de la inversión en seguridad.

Propuesta de Implementación

En esta sección continuaré utilizando el *software* de clientes Portal e-Monitor como base para el desarrollo de la propuesta de implementación técnica de los controles de seguridad de la información. Como ya se mencionó en el apartado de Análisis de Costos, la infraestructura que da soporta a este servicio está conformada por 2 servidores: uno que ejecuta la aplicación web y otro que contiene la base de datos. A los efectos de este ejercicio se entiende que estos servidores se encontrarán instalados en la nube de *Softlayer*.

Los controles técnicos de seguridad de la información a implementar en base a la matriz de controles obtenida en el análisis de riesgos son los siguientes:

- Falla de Aislamiento
- Interfaz de Administración Comprometida.
- Cuentas Administrativas
- Borrado inseguro de la información
- Transmisión insegura de datos
- Exposición a internet
- Cortes de red
- Recursos insuficientes
- Unicidad de cuentas

A continuación, se muestra un esquema de alto nivel de la infraestructura tecnológica del servicio Portal e-Monitor y de los controles de seguridad de la información.

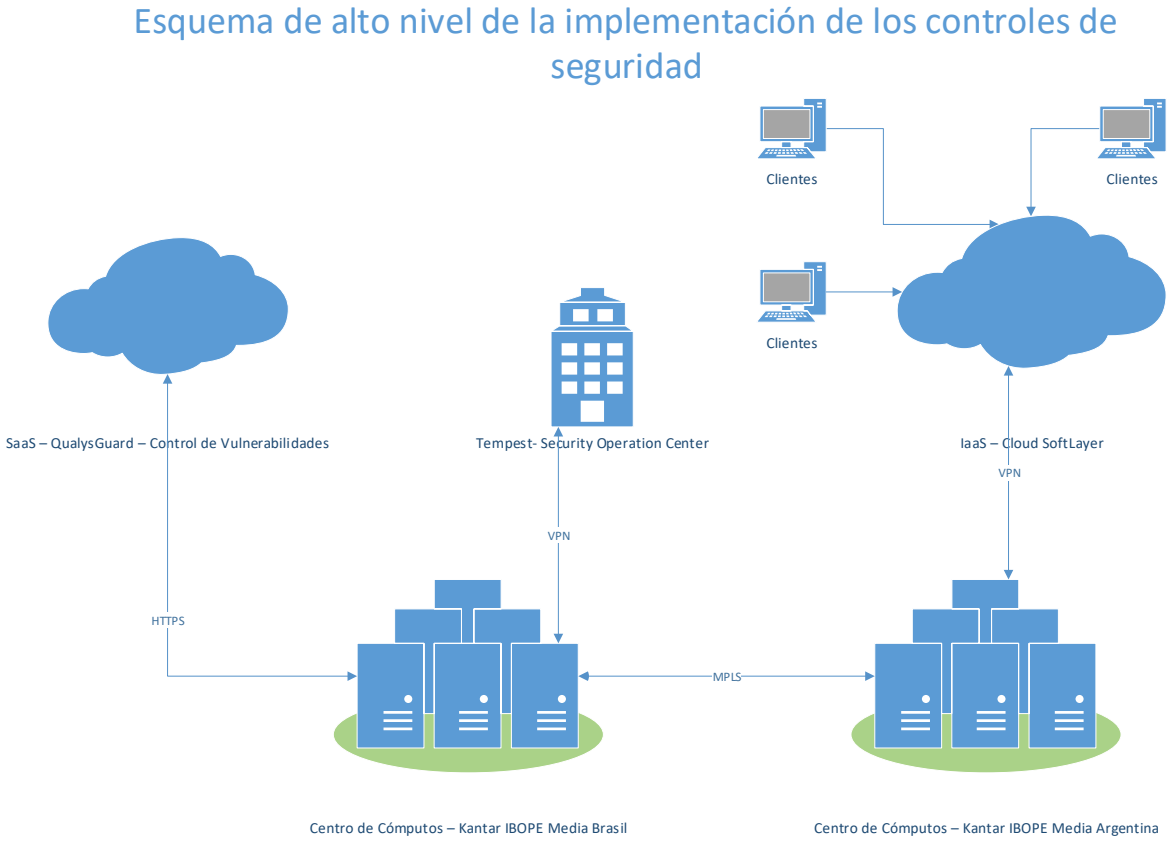


Ilustración 31 Esquema de alto nivel

Fuente: (Propia)

Tomando como referencia la clasificación de la información de esta aplicación hecha por la empresa según sus políticas, se determinó que no es necesario en este caso implementar las medidas propuestas para los controles:

- Falla de Aislamiento.
- Borrado inseguro de la información.

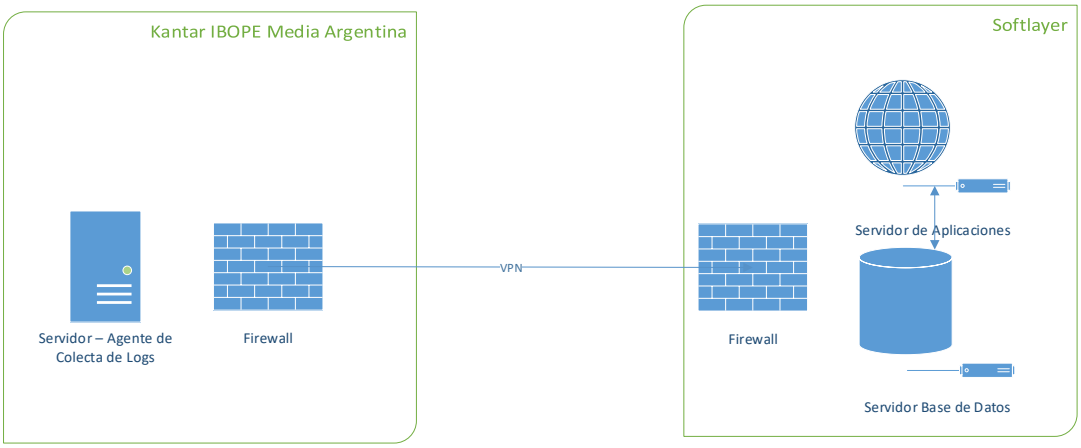
En los siguientes puntos se presenta el esquema y detalle de los controles.

Interfaz de Administración Comprometida y Transmisión insegura de datos: se deberá implementar una conexión VPN (*virtual private network* o red privada virtual) entre la red de la empresa y el servicio en la nube, de esta manera, como ya fue mencionado en el análisis

de riesgos, se acotan los puntos desde los que se pueden acceder a las interfaces de administración del entorno *cloud*. Por otra parte, con la utilización de una conexión VPN se logra que todo el tráfico que circula entre la red interna de la compañía y la nube esté encriptado de manera que será muy difícil que el mismo sea interceptado y leído por un pirata informático. Además, con el fin de proteger las credenciales y sus contraseñas de usos indebidos, las mismas deberán ser almacenadas en la herramienta *Password Manager Pro* la cuál funciona como un repositorio centralizado de contraseñas y otorga acceso a las mismas, según los permisos establecidos previamente.

Ilustración 32 Esquema VPN

Esquema de la implementación de la solución de VPN

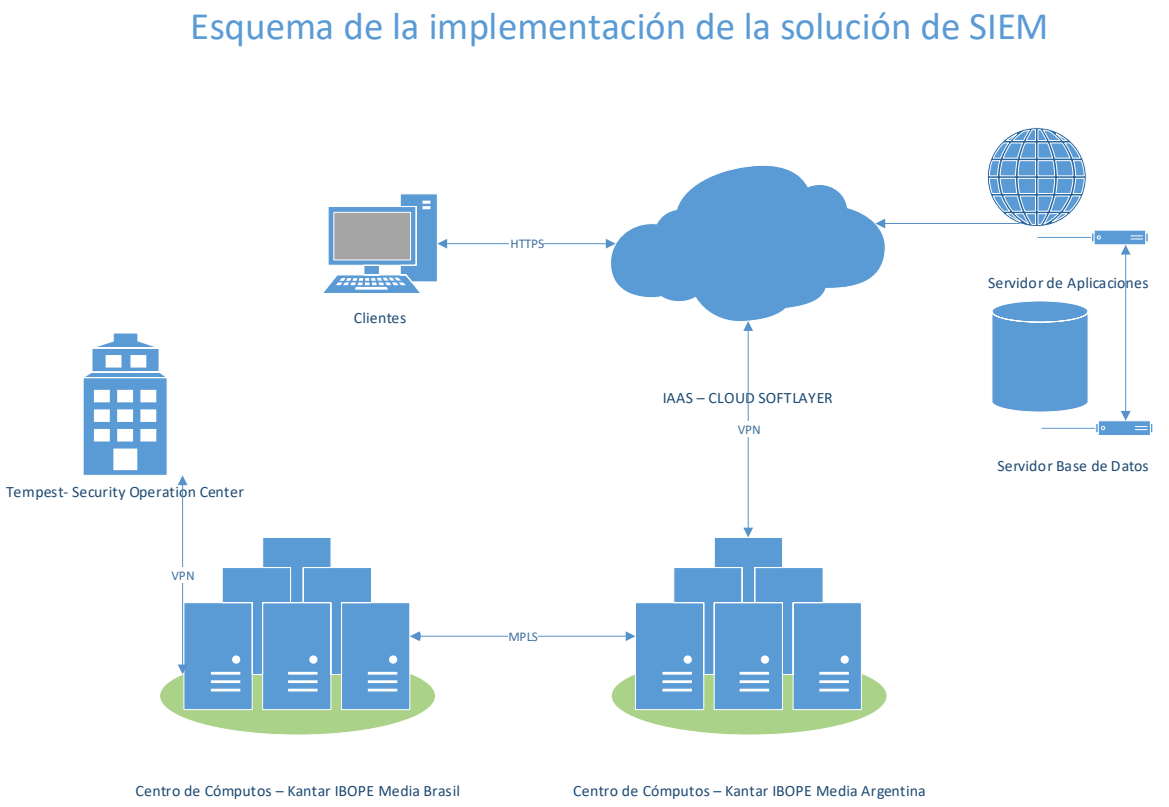


Fuente: (Propia)

Cuentas Administrativas y Exposición a internet: como ya se describió en detalle dentro del análisis de riesgos, una cuenta de usuario que posee privilegios administrativos altos puede acceder a gran parte de la información de la empresa, sino a toda, por lo que su actividad debe ser monitoreada para evitar que se vean comprometidos los activos de la información. Para esto se deberá realizar la recolección y análisis de *logs* o registros de actividad de los usuarios críticos en los servidores, aplicaciones, bases de datos y en todo dispositivo crítico. La empresa ya tiene implementada una solución de SIEM (*Security Information Event*

Management o Gestión de Eventos de Información de Seguridad) de HP llamada ArcSight por lo que sólo será necesario efectuar las configuraciones requeridas por el SIEM para poder incorporar el equipamiento de la nube. El control y monitoreo de estos registros es realizado en forma permanente por la empresa Tempest Security Intelligence mediante su servicio de SOC (*Security Operations Center* o Centro de Operaciones de Seguridad). En el siguiente gráfico se muestra en forma macro como se encuentra implementada la infraestructura de este control.

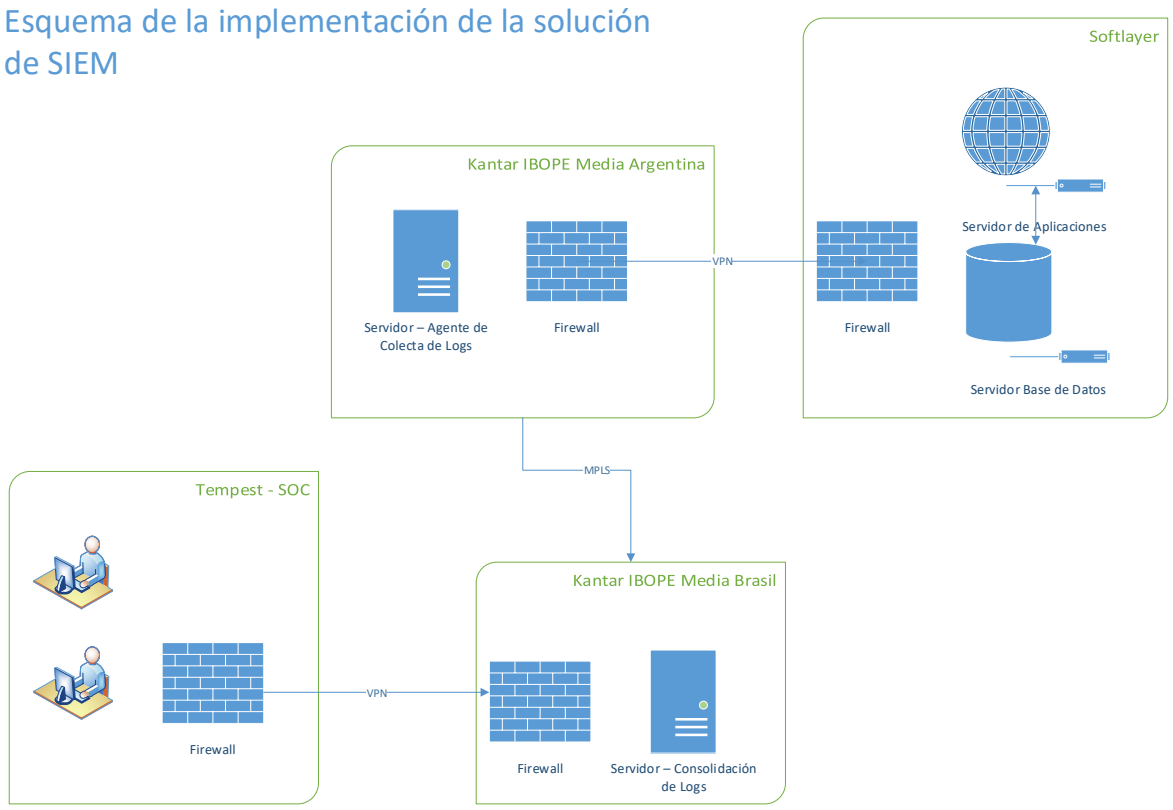
Ilustración 33 SIEM - Macro



Fuente: (Propia)

En el siguiente diagrama podemos ver en más detalle la implementación del SIEM y el servicio de SOC.

Ilustración 34 SIEM - Detalle



Fuente: (Propia)

La herramienta de SIEM se encuentra implementada en un esquema de cascada. Cada centro de cómputo de Kantar IBOPE Media tiene un servidor agente que se encarga de capturar todos los registros que generan los servidores, aplicaciones, bases de datos y dispositivos de red y enviarlos a un servidor de consolidación. Este otro servidor ubicado en el centro de cómputos de Kantar IBOPE Media en Brasil se ocupa de consolidar toda la información recibida desde cada servidor agente y controlarla de manera automática en base a determinados criterios prefijados y generar alertas en el caso que ciertos eventos se hayan registrado. A modo de ejemplo: una alerta se dispara cuando múltiples intentos de accesos erróneos a una aplicación se producen en un período muy corto de tiempo o cuando se registra el acceso a un archivo específico por parte de un usuario administrador. Esta herramienta y sus alertas son monitoreadas 7x24x365 por el servicio externo de SOC. En este caso es necesario incorporar dentro de la configuración del servidor agente, los servidores que se

encontrarán instalados en la nube para que los mismos estén dentro del circuito de monitoreo y control.

Además, como parte de los controles definidos para la mitigación del riesgo de exposición a internet se recomendó la utilización de un sistema de gestión de análisis de vulnerabilidades. La empresa ya cuenta con este servicio contratado a la compañía QualysGuard. Su implementación es relativamente sencilla ya que el mismo se encuentra contratado en modalidad SaaS (*Software as a services*) por lo que no requiere de mayores configuraciones para comenzar a funcionar que la declaración de las direcciones IP´s que van a ser escaneadas por la herramienta, la criticidad de cada IP y qué perfil de escaneo se quiere aplicar para que quede implementado. En el siguiente esquema podemos ver en forma macro cómo está instalada esta solución.

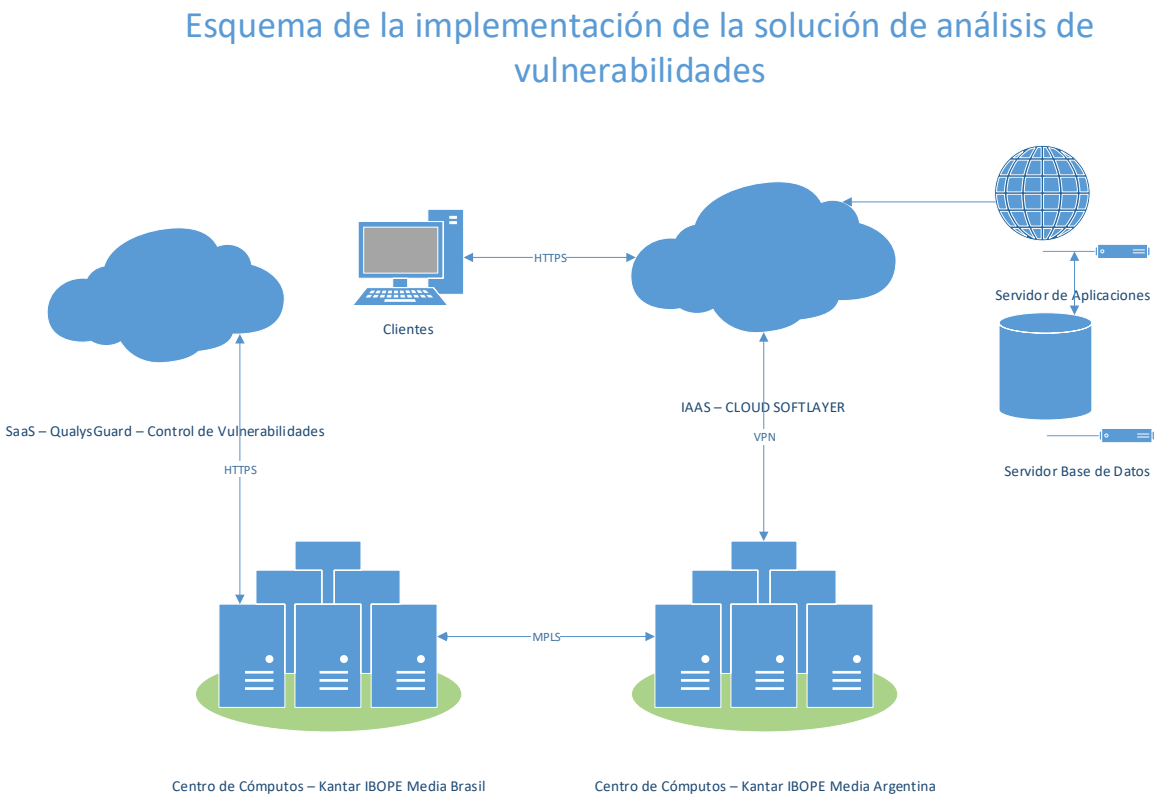
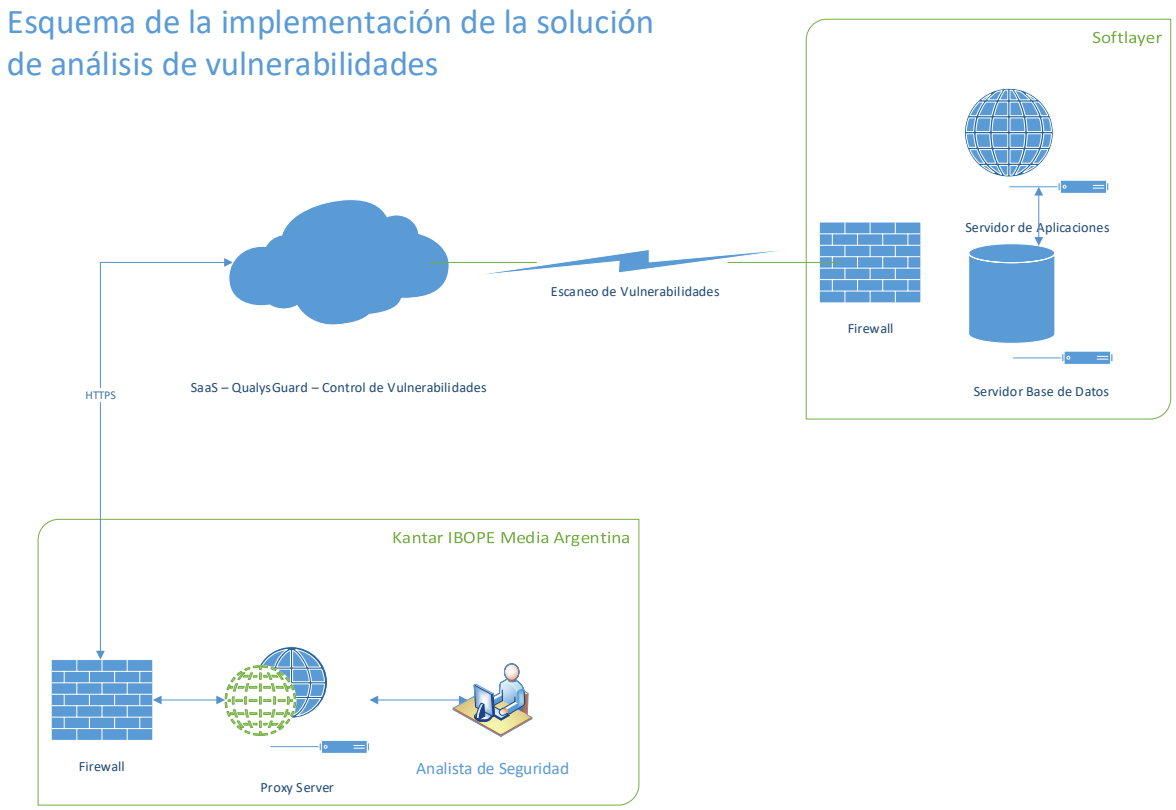


Ilustración 35 Gestión de vulnerabilidades - Macro

Fuente: (Propia)

En el próximo diagrama podemos ver como el analista de seguridad se conecta a la plataforma de Qualys y desde la misma genera la tarea de escaneo de vulnerabilidades sobre las direcciones IP´s externas del equipamiento que se encuentra instalado en la nube de *Softlayer*. Para detectar estas vulnerabilidades la aplicación de Qualys cuenta con una base de datos que le permite identificarlas durante el escaneo.

Ilustración 36 Gestión de Vulnerabilidades - Detallado



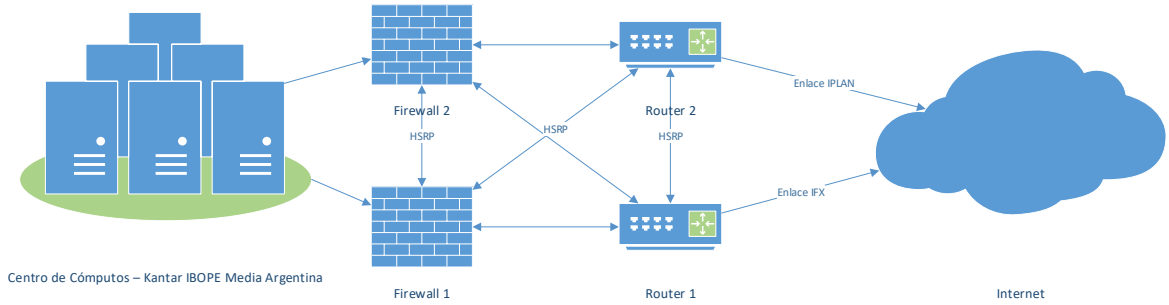
Fuente: (Propia)

Cortes de red: como ya fue explicado en el análisis de riesgos dada la naturaleza de los servicios en la nube, la conexión a internet del centro de cómputos local pasa a ser vital para la continuidad de los servicios. Es por esto que es necesario contar con un acceso a internet con alta disponibilidad. Como ya se indicó, la empresa ya cuenta con esta solución implementada y la misma puede observarse en el esquema de red que ya fue presentado en la sección de relevamiento. Este esquema cuenta con equipos *firewall* y *routers* duplicados conectados entre sí por el protocolo HSRP (*Hot Standby Router Protocol*) de CISCO. Con la utilización de este protocolo se evita la existencia de un único punto de falla en la red

mediante técnicas de redundancia. Adicionalmente se cuentan con 2 enlaces de internet de diferentes proveedores para completar el esquema de alta disponibilidad y redundancia. Por otra parte, esta infraestructura es monitoreada 7x24x365 por el NOC; en los próximos párrafos se explica en detalle cómo se encuentra implementado este control.

Ilustración 37 Esquema de alta disponibilidad

Esquema de la implementación de la solución de acceso a internet con alta disponibilidad



Fuente: (Propia)

Recursos insuficientes: otro de los riesgos identificados fue que el proveedor de servicios en la nube no brinde realmente la calidad de servicio que fue contratado. Es por esto que se recomendó en el análisis de riesgos, incorporar los equipos de la nube dentro del esquema de monitoreo de infraestructura de manera que la empresa pueda contar con una medición confiable de los servicios que le permitan verificar que el tercero está cumpliendo con los niveles de servicio contratados. Kantar IBOPE Media ya cuenta con una aplicación llamada OpManager desarrollada por la empresa ManageEngine mediante la cual es capaz de monitorear a través de agentes, el estado de los servidores, el uso del procesamiento, uso de memoria, placas de red, anchos de banda, disponibilidad, etc. Este monitoreo es realizado en un formato 7x24x365 desde un NOC (*Network Operations Center* o Centro de Control de Operaciones) que se encuentra ubicado en las oficinas de Kantar IBOPE Media Brasil. Para el caso de los controles sobre los cortes de red mencionados anteriormente, todos los

dispositivos y enlaces que permiten el acceso a internet son monitoreados por el NOC en forma activa de manera que si se presentara alguna falla o corte de servicio el mismo sería detectado en forma inmediata permitiendo una atención casi instantánea del incidente.

Esquema de la implementación de la solución de Monitoreo de Infraestructura.

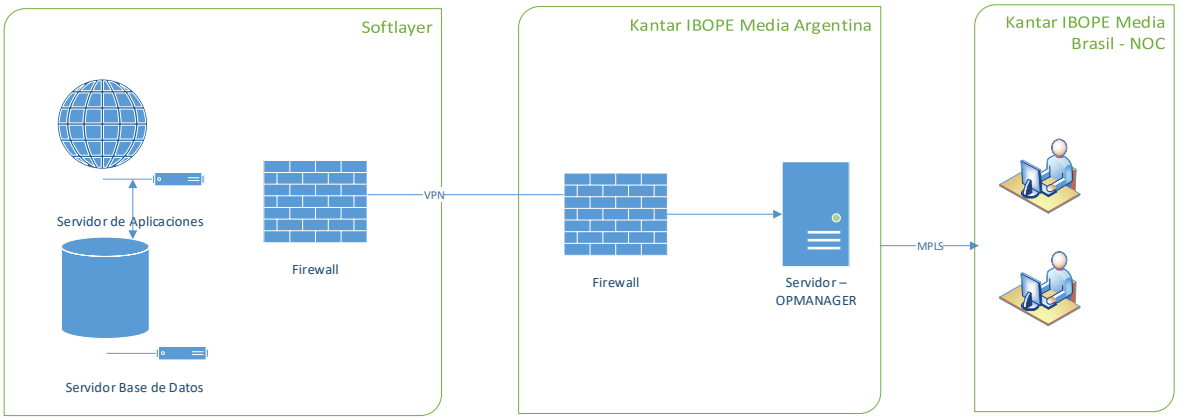


Ilustración 38 Monitoreo Infraestructura

Fuente: (Propia)

Unicidad de cuentas: el último de los controles a describir es el servicio de federación de identidades. Este tipo de aplicaciones sirven para evitar la multiplicidad de usuarios y de esta forma lograr una administración controlada y centralizada sobre todo el ciclo de vida de los usuarios. La plataforma *cloud* de Softlayer permite la integración con el *Windows Active Directory* de la compañía mediante el uso de un conector. Dicho conector permite la sincronización automática de los usuarios el *Active Directory* local y la nube; de esta forma se evita tener que dar de alta cada usuario en los dos ámbitos. En la sección T.I.C. ya fue descripto en detalle el funcionamiento de esta herramienta.

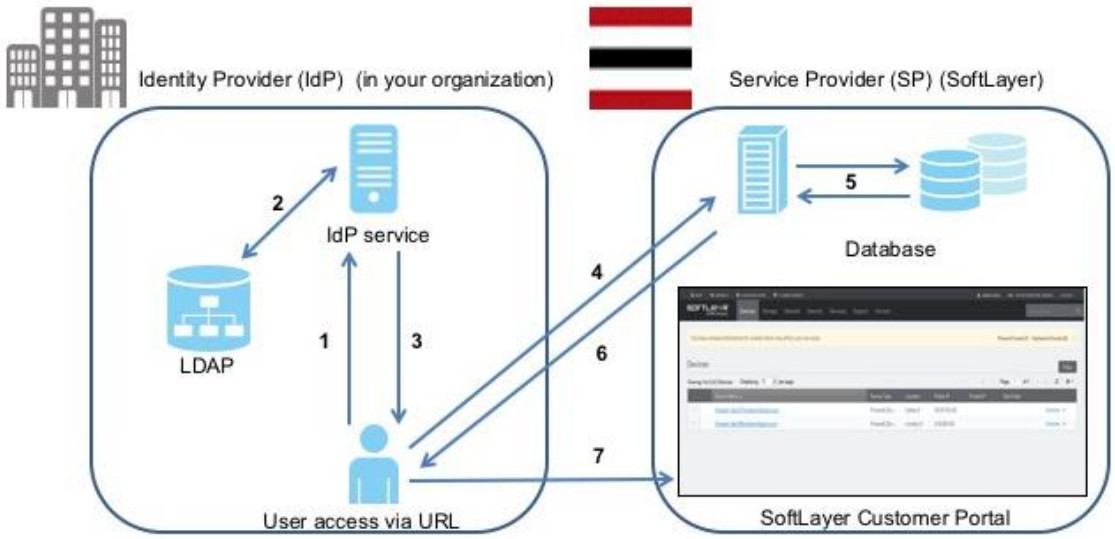


Ilustración 39 Federación

Fuente: (www.softlayer.com)

Conclusiones

Desde lo general puedo decir en que ha sido un largo y apasionante camino desde el inicio de la carrera hasta la finalización del presente trabajo. El mismo es el corolario de muchas horas de esfuerzo, estudio e investigación que finalmente han culminado.

El desarrollo de TFG ha sido realmente un desafío académico y profesional constante, un proceso sumamente interesante en la búsqueda de poder encontrar una solución a un problema, integrando lo aprendido en la mayoría de las materias. Para desarrollar este trabajo he utilizado los conocimientos adquiridos en materias como Seguridad Informática, Auditoría, Sistemas de Información, Sistemas Operativos, Arquitectura, Estadísticas, Desarrollo *Web*, Matemáticas, Liderazgo, Administración, Idiomas y Gestión de Proyectos. Es grato ver como todo lo estudiado en forma individual para cada materia ahora confluye en un mismo proyecto.

Desde lo particular, el trabajo realizado tendrá un impacto totalmente positivo dentro la empresa ya que se alcanzó el objetivo planteado al inicio de este documento, lográndose identificar las prácticas de seguridad de la información que deben ser implementadas para dar cumplimiento a los requisitos de seguridad para la utilización de un servicio en la nube; es decir, definir qué controles de seguridad son necesarios implementar para poder utilizar los entornos de *cloud computing* de forma segura.

Como se mencionó en la introducción del presente trabajo y luego fue desarrollado en mayor detalle, muchos son los riesgos a los que se enfrentan las empresas al utilizar el *cloud computing.* Sin embargo, ha quedado demostrado que si se hace un trabajo de análisis bien fundamentado y se implementan los controles necesarios es posible utilizar esta tecnología en forma segura.

Bibliografía

Garnert. (2011). ID: G00214611. Case Study: City of Los Angeles Migrates to Google Gmail.

ISACA (2012). COBIT 5. Rolling Meadows: ISACA.

Portantier, F. (2012). Seguridad Informática. Buenos Aires: RedUsers.

Harris, S. (2012). CISSP *All-in-One Exam Guide*, sexta edición. New York: McGraw-Hill Professional.

Licklider, J. (1963). *Topics for Discussion at the Forthcoming Meeting*. Washington: Advanced Research Projects Agency.

Garfinkel, S (2011). *The Cloud Imperative*. Revista MIT Technology Review. Recuperado de https://www.technologyreview.com/s/425623/the-cloud-imperative/

Gilder, G (2006). *The information factorys*. Revista WIRED. Recuperado de https://www.wired.com/2006/10/cloudware/

Mell, P. y Grance, T. (2011). NIST Special Publication 800-145: *The NIST Definition of Cloud Computing*. National Institute of Standards and Technology. Recuperado de http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

IBM (2018). IaaS PaaS SaaS - *Cloud Service Models*. Recuperado de https://www.ibm.com/cloud-computing/learn-more/iaas-paas-saas/

AWS (2018). Soluciones en la nube. Recuperado de https://aws.amazon.com/es/solutions/

ENISA (2018). *Cloud Computing Certification*. Recuperado de https://resilience.enisa.europa.eu/cloud-computing-certification

OSWAP (2018). *Cloud Top 10 Security Risks*. Recuperado de: https://www.owasp.org/index.php/Category:OWASP_Cloud_%E2%80%90_10_Project

GDPR (2018). *General Data Protection Regulation*. Recuperado de: https://www.eugdpr.org/

Ley Patriótica (2018). *The USA Patriot Act*. Recuperado de: https://www.justice.gov/archive/ll/highlights.htm

Modulo (2018). Gestão de Riscos e Vulnerabilidades de TI. Recuperado de http://www.modulo.com.br/gestao-de-riscos-e-vulnerabilidades-de-ti/

OSWAP (2018). *The Open Web Application Security Project*. Recuperado de: https://www.owasp.org/index.php/Main_Page

ISO (2018). *International Organization for Standardization*. Recuperado de: https://www.iso.org/home.html

ISACA (2018). COBIT 5 Home Page. Recuperado de: http://www.isaca.org/cobit/pages/default.aspx

Qualys (2018). QualysGuard *Vulnerability Management*. Recuperado de: https://www.qualys.com/qualysguard/

Harris, S. y Maymí, F. (2016) CISSP All-in-One Exam Guide, séptima edición. New York: McGraw-Hill Professional.

HP (2018). ArcSight *Enterprise Security Manager* (ESM). Recuperado de: https://software.microfocus.com/en-us/products/siem-security-information-event-management/overview

ManageEngine (2018). *Softwares*: *Password Manager* Pro y OpManager. Recuperado de: https://www.manageengine.com/latam/

SoftLayer (2018). Cloud Services. Recuperado de: http://www.softlayer.com/

Garnert. (2016). *Magic Quadrant for Cloud Computing*.

Ley 25.326 (2000). Protección de los Datos Personales. Recuperado de: http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm

MAGERIT (2012). MAGERIT: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Versión 3. España. Ministerio de Hacienda y Administraciones Públicas.

ISACA (2014). Manual de preparación al examen CRSIC 2014. Rolling Meadows: ISACA.

NIST (2012). NIST Special Publication 800-30 Revision 1: Guide for Conducting Risk Assessments. Recuperado de: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

ENISA (2009). Computación en la nube: Beneficios, riesgos y recomendaciones para la seguridad de la información. Recuperado de: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/files/deliverables/cloud-computing-risk-assessment-spanish

Cloud Security Alliance (2018). Cloud Controls Matrix. Recuperado de: https://cloudsecurityalliance.org/group/cloud-controls-matrix/#_overview

HIMSS (2018) *Cloud Security Toolkit*. Recuperado de: http://www.himss.org/library/healthcare-privacy-security/cloud-security/toolkit

Sonnenreich, W. (2005) *Return On Security Investment* (ROSI): A Practical Quantitative Model. New York: SageSecure.

ANEXO E – FORMULARIO DESCRIPTIVO DEL TRABAJO FINAL DE GRADUACIÓN

AUTORIZACIÓN PARA PUBLICAR Y DIFUNDIR TESIS DE POSGRADO O GRADO A LA UNIVERIDAD SIGLO 21

Por la presente, autorizo a la Universidad Siglo21 a difundir en su página web o bien a través de su campus virtual mi trabajo de Tesis según los datos que detallo a continuación, a los fines que la misma pueda ser leída por los visitantes de dicha página *web* y/o el cuerpo docente y/o alumnos de la Institución:

Autor-tesista *(apellido/s y nombre/s completos)*	Pi, Pablo Lionel
DNI *(del autor-tesista)*	24227149
Título y subtítulo *(completos de la Tesis)*	Computación en la nube, controles de seguridad
Correo electrónico *(del autor-tesista)*	pi_74@yahoo.com
Unidad Académica *(donde se presentó la obra)*	Universidad Siglo 21

Otorgo expreso consentimiento para que la copia electrónica de mi Tesis sea publicada en la página web y/o el campus virtual de la Universidad Siglo 21 según el siguiente detalle:

Texto completo de la Tesis *(Marcar SI/NO)*[1]	SI
Publicación parcial *(Informar que capítulos se publicarán)*	

Otorgo expreso consentimiento para que la versión electrónica de este libro sea publicada en la página web y/o el campus virtual de la Universidad Siglo 21.

Lugar y fecha: _____

_____ _____

Firma autor-tesista **Aclaración autor-tesista**

Esta Secretaría/Departamento de Grado/Posgrado de la Unidad Académica:

_____certifica que la tesis adjunta es la aprobada y registrada en esta dependencia.

_____ _____

Firma Autoridad Aclaración Autoridad

Sello de la Secretaría/Departamento de Posgrado

[1] Advertencia: Se informa al autor/tesista que es conveniente publicar en la Biblioteca Digital las obras intelectuales editadas e inscriptas en el INPI para asegurar la plena protección de sus derechos intelectuales (Ley 11.723) y propiedad industrial (Ley 22.362 y Dec. 6673/63. Se recomienda la NO publicación de aquellas tesis que desarrollan un invento patentable, modelo de utilidad y diseño industrial que no ha sido registrado en el INPI, a los fines de preservar la novedad de la creación.