ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

MODELO DE GESTIÓN DE RIESGOS DE INFRAESTRUCTURA COMO SERVICIOS (IaaS) DE CLOUD COMPUTING PARA EMPRESAS DEL SECTOR PÚBLICO ECUATORIANO.

TESIS PREVIO A LA OBTENCIÓN DEL TÍTULO DE MÁSTER EN GESTIÓN DE LAS COMUNICACIONES Y TECNOLOGÍAS DE LA INFORMACIÓN

GUILLERMO OSWALDO MOROCHO LLIVICOTA
danny_morocho@hotmail.com

DIRECTOR: Msc. DENYS ALBERTO FLORES ARMAS
denys.flores@epn.edu.ec

Quito, Diciembre 2015

DECLARACIÓN

Yo, Guillermo Oswaldo Morocho Llivicota, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

Guillermo Oswaldo Morocho Llivicota

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Guillermo Oswaldo Morocho Llivicota, bajo mi supervisión.

Msc. DENYS FLORES
DIRECTOR DE PROYECTO

AGRADECIMIENTOS

Quiero dejar constancia de mi profundo y sincero agradecimiento a la Escuela Politécnica Nacional por sus extraordinarios profesores que me han guiado por el camino del conocimiento y profesionalismo.

Mi agradecimiento especial al Ing. Denys Flores por su valioso tiempo y aporte en el desarrollo de este trabajo, ya que sin su ayuda y desinteresada colaboración todo este trabajo habría sido imposible de realizar.

A la Dirección de Tecnologías de la Información y Comunicación de la Agencia Nacional de Tránsito, en especial al Ing. Humberto Guerrero, por su confianza y apoyo incondicional que hizo posible la realización de este trabajo.

Guillermo Morocho

DEDICATORIA

A dios que me da la oportunidad de vivir y por bendecirme para llegar a donde he llegado.

A mi padre, por estar siempre en los momentos importantes de mi vida, por ser el ejemplo para salir adelante y por los consejos que han sido de gran ayuda para mi vida y crecimiento. Esta tesis es el resultado de lo que me has enseñado en la vida, ya que siempre has sido una persona honesta, entregada a tu trabajo, y un gran líder, pero más que todo eso, una gran persona que siempre ha podido salir adelante y ser triunfador. Es por ello que hoy te dedico este trabajo de tesis. Gracias por confiar en mí y darme la oportunidad de culminar esta etapa de mi vida.

A mi Abuela, que con la sabiduría de Dios me has enseñado a ser quien soy hoy. Gracias por tu paciencia, por enseñarme el camino de la vida, gracias por tus consejos, por el amor que me has dado y por tu apoyo incondicional en mi vida. Gracias por llevarme en tus oraciones porque estoy seguro que siempre lo haces.

A mi Madre, por ser la amiga y compañera que me ha ayudado a crecer, gracias por estar siempre conmigo en todo momento. Gracias por la paciencia que has tenido para enseñarme, por el amor que me das, por tus cuidados en el tiempo que hemos vivido juntos, por los regaños que me merecía y que no entendía. Gracias Mamá por estar al pendiente durante toda esta etapa

A mis hermanas Anita y Norma, que con su amor me han enseñado a salir adelante. Gracias por su paciencia, gracias por preocuparse por su hermano varón, gracias por compartir sus vidas, pero sobre todo, gracias por estar en otro momento tan importante en mi vida.

A mi amiga y compañera, por su paciencia, perseverancia y constancia, gracias por presionarme para terminar este trabajo, gracias por ayudarme con la correcciones, gracias por aguantarme, pero sobre todo gracias por enseñarme a creer en mí y motivarme hacer la cosas de mejor manera.

A Denys Flores, director y tutor de tesis, docente universitario que en los momentos difíciles estuvo ahí para ayudarme. Gracias por sus consejos, conocimientos y experiencia y por su valioso tiempo dedicado a este trabajo de tesis.

Gracias a todos aquellos que no están aquí, pero que me ayudaron a que este gran esfuerzo se volviera realidad.

Guillermo Morocho Llivicota

CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El vertiginoso desarrollo e innovación de las tecnologías de la información en los últimos años ha permitido que la mayoría de organizaciones en el mundo este a la vanguardia tecnológica con el menor esfuerzo e inversión posible, esto gracias al paradigma tecnológico de Computación en Nube, no obstante se está dejando de lado los principios básico de la Seguridad de la Información que deberían tomarse en cuenta durante todo proceso de externalización de infraestructura, plataforma o aplicación, más aún cuando en el ámbito local, no existe normativa legal que la regule.

El presente proyecto, pretende sentar las bases y ser el primer frente para la Gestión de Riesgos de Servicios de Cloud Computing en entidades del sector público ecuatoriano.

El documento se encuentra dividido en 4 capítulos. El primer capítulo corresponde al análisis de la situación actual de la Seguridad de la Información basada en un enfoque de gestión de riesgos de servicios de Cloud Computing tanto en el mercado nacional como internacional, a fin de identificar los principales problemas y posibles soluciones para una adopción exitosa de este nuevo paradigma de TI llamado Cloud Computing por parte de las entidades del sector público ecuatoriano.

El segundo capítulo corresponde al desarrollo del Modelo de Gestión de Riesgos de Servicios de Cloud Computing basados en los marcos de trabajo COBIT, OCTAVE e ISO27000; para lo cual se realizará un análisis de estos marcos de trabajos a fin de establecer la estrategia de integración de la estructura de COBIT con las fases, procesos y actividades de OCTAVE y los Objetivos de Control y Controles de la ISO 27000, lo que nos conllevará a la determinación de controles para la mitigación de los potenciales riesgos que implicaría la adopción o migración a la nube por parte de las entidades del sector público ecuatoriano.

En el tercer capítulo se realiza la validación del modelo en un caso de estudio cuyos resultados serán puestos a consideración de la alta directiva, quiénes bajo su mejor criterio, dispondrá la aplicación del modelo como un marco de trabajo guía en el análisis, evaluación y mitigación de potenciales riesgos de los servicios de Cloud Computing.

Finalmente en el capítulo cuarto se presentan las respectivas conclusiones y recomendaciones, obtenidas a lo largo del desarrollo del presente proyecto de titulación.

PRESENTACIÓN

La Computación en la Nube como modelo que facilita una red ubicua, conveniente y bajo demanda para compartir un conjunto de recursos informáticos configurables que se pueden asignar rápidamente y desplegar con un esfuerzo mínimo de gestión [1] brinda innumerables beneficios. Sin embargo, hay que tener en cuenta que junto con los beneficios vienen riesgos y preocupaciones de seguridad, más aún cuando recientes revelaciones sobre espionaje político y empresarial [2], están obligando a países como el gobierno ecuatoriano a implementar medidas de seguridad que mitiguen los potenciales riesgos que implicaría adoptar Cloud Computing [3] como un nuevo modelo de TI por parte de las entidades del sector público.

Está claro, que la computación en la nube al ser una tecnología emergente no se puede garantizar una total protección de la información, pero mediante la incorporación de normas, estándares y mejores prácticas de TI existentes para la gestión de la seguridad de la información se puede identificar, gestionar, minimizar y asumir los potenciales riesgos que pueden atentar contra las entidades públicas ecuatorianas de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en el entorno y las tecnologías, fruto de la adopción de la Nube.

Considerando que en el Estado ecuatoriano aún no se dispone de una normativa legal que regule los servicios de Cloud Computing, y que ésta se vislumbra como solución plausible para cualquier empresa o entidad pública, el presente trabajo tiene como finalidad desarrollar un Modelo de Gestión de Riesgos de Infraestructura como Servicios (IaaS) de Cloud Computing aplicado a entidades del sector público ecuatoriano, que sirva como marco de trabajo en la identificación, evaluación y mitigación de riesgos, basándose para ello en normas, estándares y mejores prácticas existentes. Modelo de gestión de riesgos que será aplicado como caso de estudio a la Agencia Nacional de Tránsito.

PLANTEAMIENTO DEL PROBLEMA

Hoy en día las garantías y niveles de servicios ofrecidos por los mejores operadores en el mercado de Cloud Computing están permitiendo a entidades públicas y empresas ecuatorianas alojar datos sensibles en la Nube [4], sin embargo, casos recientes nos recuerda la criticidad en el manejo de la seguridad de la información [2].

Dado que la seguridad de la información es uno de los aspectos críticos que más preocupa al área de Tecnologías de la Información para la adopción general de los servicios en Nube, ya que implica confiar su principal activo a un tercero (Cloud Service Providers - CSP), la mayoría de entidades y/o empresas toman medidas que garanticen el control de su información y que mitiguen los potenciales riesgos que la puedan impactar [3]. Para ello utilizan herramientas o marcos de trabajo existentes, que originalmente fueron pensados para ambientes de computación tradicional, por lo tanto, un poco inadecuados con este nuevo modelo de Computación en la Nube; ya que por ejemplo, tanto los procesos como la infraestructura y la información pueden estar alojados en las instalaciones del CSP, bajo la legislación de otro país [5], criterios no contemplados inicialmente por parte de las normas para el aseguramiento de la información.

De acuerdo al Sistema Integrado de la Legislación Ecuatoriana eSilecPro [6], en el ámbito nacional el Estado ecuatoriano no dispone de normativa legal vigente que regule los servicios en la Nube provistos por un CSP, mientras que en el ámbito internacional, según la Organización Internacional de Normalización (ISO) [7] y estudios realizados por Gartner [2], los estándares de seguridad en la Nube están comenzando a tener una gran expectativa en el mercado, pero solo estarán listos dentro de un par de años, dejando un vacío que los estándares o mejores prácticas actuales no cubren.

Al identificar entonces que en el Estado ecuatoriano no se dispone de una normativa legal o modelo de referencia para la gestión de la seguridad de la información en la Nube, en este trabajo se propone un Modelo de Gestión de Riesgos para la adopción de la computación en nube por parte de las entidades del sector público ecuatoriano. Modelo de gestión de riesgos, que será el resultado de integrar los marcos de trabajo COBIT, OCTAVE e ISO 27000, para ser aplicados como caso de estudio a la Agencia Nacional de Tránsito (ANT).

OBJETIVOS

GENERAL

Desarrollar un Modelo de Gestión de Riesgos de Infraestructura como Servicios (IaaS) de Cloud Computing para ser aplicado a entidades del sector público ecuatoriano, basados en los marcos de trabajo COBIT, OCTAVE e ISO27000, que sirva de apoyo a la alta directiva en el proceso de implementación de este nuevo modelo de servicios.

ESPECÍFICOS

- Especificar el estado del arte de estándares, modelos y mejores prácticas relacionadas con la Gestión de Riesgos de Servicios de Cloud Computing.
- Establecer una estrategia de integración de estándares, modelos y buenas prácticas seleccionadas para la Gestión de Riesgos de Servicios de Cloud Computing aplicado a entidades del sector público ecuatoriano.
- Especificar un nuevo Modelo de Gestión de Riesgos de Servicios de Cloud Computing aplicado a entidades del sector público ecuatoriano.
- Validar el modelo mediante la aplicación a un caso de estudio.

DESTINATARIOS

- Directores Ejecutivos (CEO), Directores de Tecnología de la Información (CIO), Directores de Seguridad de la Información (CISO) y demás personal involucrado con las Tecnologías de la Información y Comunicación, que consideran a la gestión de riesgos como un requisito previo frente a una posible adopción de la computación en la Nube.
- Entidades de la Administración Pública Central, Institucional y Dependiente de la Función Ejecutiva preocupados del análisis costo beneficio que conllevaría una posible migración de toda o parte de su infraestructura, plataforma o aplicaciones hacia la Nube.
- Responsables de expedir, codificar, reformar y derogar leyes o políticas públicas que regulen y normen la incorporación de Computación en la Nube por parte de los gobiernos y administraciones públicas.

- Proveedores de nube y/o servicios de valor añadido que deseen obtener una primera idea acerca de las necesidades y requisitos de las entidades de la Administración Pública Central, Institucional y Dependiente de la Función Ejecutiva.

CAPITULO 1

ESTUDIO DEL ESTADO DEL ARTE DE LA GESTIÓN DE RIESGOS DE SERVICIOS DE CLOUD COMPUTING.

La necesidad por satisfacer las crecientes demandas de TI, está impulsando a muchas organizaciones del mundo a examinar de cerca la computación en la nube como una opción real a sus necesidades organizacionales. Para ISACA [8] la promesa de una computación en la nube está revolucionando el mundo de servicios de TI al transformar la computación en una unidad ubicua, al sacar provecho de atributos tales como mayor agilidad, elasticidad, capacidad de almacenamiento y redundancia para gerenciar activos de información. Todo esto gracias a la influencia continua y el uso innovador de Internet que está permitiendo que la computación en la nube utilice la infraestructura existente y la transforme en servicios que podrían proporcionar a las organizaciones tanto ahorros significativos en costos como aumento en la eficiencia. Las organizaciones están descubriendo que hay un potencial en aprovechar esta innovación para prestar un mejor servicio a los usuarios y obtener ventajas de negocio.

Según el último estudio del Estado de la Seguridad en Cloud Computing de la Cloud Security Alliance [9], en lo que va del 2014 se ha evidenciado un incremento en el uso de la computación en la nube, ya que ofrece a las organizaciones la oportunidad de separar sus necesidades de TI y su infraestructura, lo que a la postre se traduce en ahorros en TI a largo plazo, incluyendo reducción de costos de infraestructura y modelos de pago por servicio.

Como enfatiza el NITS [10], el traslado de servicios de TI a la nube permite a las organizaciones aprovechar el uso de servicios en un modelo por demanda, lo que requiere un menor gasto inicial de capital con un alto grado de flexibilidad a los negocios con nuevos servicios de TI.

Por lo tanto, es innegable qué la computación en la nube se está convirtiendo en una atractiva oferta para la provisión de servicios para cualquier organización que busca mejorar sus recursos de TI al tiempo que controla sus costos. Sin embargo,

hay que tener en cuenta que junto con los beneficios vienen riesgos y preocupaciones de seguridad que debe considerarse [11], más aún si se pretende contratar servicios de TI fuera de la organización, ya que existe un riesgo agregado de mayor dependencia de un tercero que proporcione servicios de TI flexibles, disponibles, resilientes y eficientes. Aunque la mayoría de organizaciones están acostumbradas a gestionar este tipo de riesgos internamente, se requieren cambios para expandir los enfoques y las estructuras de gobierno a fin de manejar apropiadamente las nuevas soluciones de TI y mejorar los procesos de negocio.

Al igual que ocurre con cualquier tecnología emergente, la computación en la nube ofrece la posibilidad de obtener una alta recompensa en lo que respecta a contención de costos y características como agilidad y velocidad de suministro. Sin embargo, como una "nueva" iniciativa, también puede traer consigo un posible riesgo alto. La computación en la nube introduce un nivel de abstracción entre la infraestructura física y el propietario de la información que se almacena y se procesa. Tradicionalmente, el propietario de los datos ha tenido control directo o indirecto del entorno físico que afecta sus datos. En la nube, éste ya no es el caso. Debido a esta abstracción, ya existe una demanda ampliamente generalizada de mayor transparencia y un enfoque de seguridad robusto del ambiente de seguridad y control del proveedor de computación en la nube por parte del propietario de la información.

Una vez que se ha determinado que los servicios en la nube son una solución plausible para una organización, es importante identificar los objetivos y riesgos para el negocio que acompañan a la nube, lo que nos permitirá determinar qué tipo de datos de la nube son confiables, así como cuáles servicios podrían ofrecer el mayor beneficio.

1.1 CLOUD COMPUTING COMO ESTRATEGIA GUBERNAMENTAL

Grandes corporaciones de TI como Amazon, CloudFlare, OVH y SoftLayer (IBM), así como gobiernos de países de la Unión Europea, Norte América, Asia y América Latina, ver Figura 0.1, están proveyendo e impulsando la adopción de la computación en la nube como una estrategia gubernamental para el crecimiento

económico sostenible, la innovación y el coste-eficacia de los servicios públicos y para transformar el uso de las Tecnologías de la Información en beneficio de la ciudadanía a fin de incrementar sus niveles de calidad y servicios [12].

Figura 0.1 Popularidad y localización por continente de Cloud Provider [13].

Mediante la adopción de la computación en la nube los gobiernos buscan aprovechar la infraestructura, las plataformas o los servicios de software que ofrecen los proveedores para externalizar sus servicios internos. Este cambio sustancial en el modo de adquirir y gestionar la tecnología puede someter a un estado al igual que a cualquier organización a cierta tensión que sin un enfoque adecuado, pueden exponerla a un mayor nivel de riesgo, más aún, si su estructura, cultura, políticas, prácticas y arquitectura no han evolucionado para adaptarse a la computación en la nube.

1.1.1 DEFINIENDO COMPUTACIÓN EN LA NUBE

Actualmente existe una diversidad de definiciones del concepto de computación en la nube ya sea desde el punto de vista del proveedor o usuario, modelo de servicio o implementación, sin embargo, la que goza de mayor aceptación es la que ha presentado el Instituto Nacional de Normas y Tecnología (NIST, National Institute of Standards and Technology) de los EE. UU., que la define como “un modelo que permite obtener, desde cualquier lugar y bajo demanda, un cómodo acceso a través de una red a un conjunto (pool) compartido de recursos informáticos configurables, el cual se puede conformar y suministrar rápidamente con un esfuerzo de gestión mínimo o con una interacción mínima con el proveedor de los servicios.” [1]

Otra definición que va tomando fuerza por parte de los países de la Unión Europea es la de la Cloud Security Alliance (CSA), que la define como “un modelo a la carta

para la asignación y el consumo de computación, a través de la cual se puede utilizar una serie de servicios, aplicaciones, información e infraestructura compuesta por reservas de recursos de computación, redes, información y almacenamiento. Estos componentes pueden orquestarse, abastecerse, implementarse y desmantelarse rápidamente, y escalarse en función de las dimensiones para ofrecer unos servicios de tipo utilidad.” [9]

Para la Comisión Europea la computación en la nube puede entenderse como “el almacenamiento, tratamiento y utilización de datos en ordenadores a distancia a los que se tiene acceso a través de Internet. Esto significa que los usuarios pueden obtener una capacidad informática casi ilimitada y a voluntad, que no tienen que hacer importantes inversiones de capital para satisfacer sus necesidades y que pueden acceder a sus datos desde cualquier lugar con una conexión a Internet. La computación en la nube tiene potencial para reducir considerablemente los gastos informáticos de los usuarios y para que se desarrollen muchos servicios nuevos. Utilizando la nube, hasta las más pequeñas organización pueden llegar a mercados cada vez mayores, y las administraciones públicas pueden hacer sus servicios más eficientes y atractivos, a la vez que contienen el gasto.” [14]

Si bien estas definiciones expone eficazmente las características esenciales de la computación en la nube, se limitan a describir este concepto en su forma más básica, ya que no aborda otros aspectos igualmente importantes sobre cómo se usa la computación en la nube dentro de las organizaciones o en qué se distingue de otras soluciones tecnológicas o de otros mecanismos de suministro, lo que genera cierta tensión que las organizaciones deben tener en cuenta y comprender, si desean estar mejor preparadas para gobernar y administrar con mayor eficacia las soluciones en la nube suministradas a nivel interno y externo, así como para integrar la nube con la estrategia gubernamental.

La adopción y el uso de la computación en la nube evolucionan a medida que las organizaciones adquieren experiencia en el aprovechamiento de infraestructuras, plataformas y servicios de software. Dado que las ofertas en la nube se revisan y mejoran para cubrir necesidades cambiantes, los líderes en materia de negocios y tecnología necesitarán orientación para asegurarse de que el valor puede ser obtenido y la confianza puede estar asegurada, no siendo la excepción las

entidades gubernamentales, que requieren orientación y recursos relacionados con la seguridad de la información, el aseguramiento de los sistemas de información, la gestión de riesgos y el cumplimiento normativo; objetivo principal del presente proyecto.

Al respecto, según la guía de Buenas Prácticas Para Desplegar Nubes Gubernamentales De Forma Segura (Good Practice Guide for securely deploying Governmental Clouds) [15], publicada por la Agencia Europea de Seguridad de las Redes y de la Información (ENISA), se identificas las siguientes características que definen a una Nube Gubernamental:

- Una Nube Gubernamental es un entorno de ejecución de servicios que cumplen con las legislaciones en materia de seguridad, privacidad y recuperación (***Qué?***)
- Una Nube Gubernamental es una forma segura y confiable (nube privada o nube pública) para ejecutar los servicios bajo la gobernanza del organismo público (***¿Cómo?***)
- Una Nube Gubernamental es un modelo para construir, implementar y entregar servicios de TI a las entidades gubernamentales (entrega interna de los servicios), a los ciudadanos y a las empresas (entrega externa de servicios a la sociedad) (***¿para qué?***)

Características que en complemento de la NIST definen una nube gubernamental como: “Más que una plataforma centralizada basada en tecnologías de virtualización, que ejecuta servicios de gobierno electrónico y cumple con las características antes mencionadas; Modelo de negocio gubernamental que permite la estandarización de servicios y SLA’s, para ahorrar costos y ayudar a la sociedad; Modelo de despliegue que provea servicios básicos (autenticación, almacenamiento, gestión de documentos, gestión de flujo de trabajo) para ser utilizado tanto por sus entidades gubernamentales y ministerios como por la ciudadanía y empresas privadas (sociedades) mediante la construcción de servicios de gobierno electrónico [15]”. Definición que está siendo adoptada por países de la Unión Europea encabezados por España, Reino Unido y Francia, países pioneros e innovadores en el despliegue de infraestructura de computación

en la nube para el Sector Público o de Gobierno, como solución más económica y segura para la protección de los datos de los ciudadanos.

Por lo expuesto se evidencia que un servicio en la nube debe caracterizarse por la abstracción al usuario final respecto a procesos de adquisición, configuración y administración de la infraestructura, plataforma o aplicación utilizada por el proveedor para la entrega de servicios de TI. Bajo este modelo se satisface cualquier necesidad de capacidad y rendimiento de forma totalmente escalable y modulable, flexibilizando el coste en función del uso que se haga de dichos servicios. [16]

1.1.2 MODELOS DE SERVICIOS, PROVISIÓN Y CARACTERÍSTICAS

De acuerdo al último informe de ISACA sobre los “Beneficios De Negocio Con Perspectivas De Seguridad, Gobierno Y Aseguramiento”, se puede pensar en el modelo de nube como un diseño compuesto por tres modelos de servicio, cuatro modelos de implementación y cinco características esenciales, misma que se pueden resumir en el cubo de la Figura 1.1.3.1, donde los riesgos y beneficios generales diferirán según el modelo de servicio e implementación, a las cuales las organizaciones deben hacer frente.

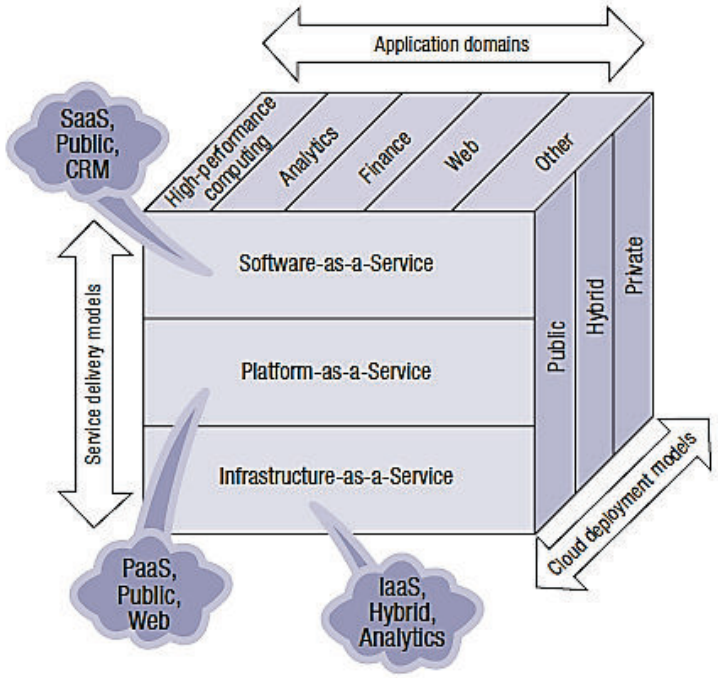

Figura 1.1.3.1 Modelo de servicio, implementación y características esenciales de computación en la nube [12].

Desde la perspectiva de prestación de servicios la computación en la nube se la puede categorizar en [17]:

- ***Infraestructura como Servicio (IaaS - Infrastructure as a Service)***.- En este modelo de servicios el proveedor entregaría a las entidades públicas la infraestructura básica de computo (procesamiento, almacenamiento y equipamiento de red) para que haga uso de estos recursos para el despliegue y ejecución de software, sistemas operativos y aplicaciones como: base de datos, alojamiento Web, entornos de desarrollo de aplicaciones, servidores de aplicaciones, streaming de video y otros. La ventaja al utilizar este modelo es que la entidad pública evita la adquisición y despilfarro de recursos de TI. Siendo responsabilidad del proveedor garantizar su funcionamiento mediante la implementación de medidas ambientales, respaldo eléctrico, sistema de prevención y extinción de incendios, sistema de protección de la seguridad física, etc., que normalmente una entidad pública con asignación presupuestaria limitado no posee. En este modelo de servicios el proveedor está a cargo de la Infraestructura, pero es la entidad pública quien está a cargo de las aplicaciones, por lo tanto él deberá encargarse de la seguridad lógica de sus datos y de sus sistemas. Casos de éxito: Amazon Web Services, CloudFare, OVH y SoftLayer (IBM).

- ***Plataforma como Servicio (PaaS – Platform as a Service)***.- Este modelo propone ofrecer a la entidad publica un conjunto de herramientas y SDK para el desarrollo de software y aplicaciones Web. En este modelo a más de evitar la adquisición de hardware como servidores, respaldos eléctricos, equipos de seguridad, también prescinde de la instalación de sistemas operativos, sistemas de bases de datos y servidores de aplicaciones, ya que todo esto viene incluido en la plataforma del proveedor. La entidad pública no gestiona la infraestructura donde correrán las aplicaciones, pero tiene total dominio sobre ellas, así la administración de las aplicaciones situadas en el entorno PaaS es más sencilla que en un entorno tradicional. La principal ventaja de este servicio es que los desarrolladores de software pueden tener fácil accesibilidad a la programación de las aplicaciones, independientemente de la ubicación geográfica, debido a que el acceso se lo realiza mediante la Internet. PaaS viene a remplazar al hosting tradicional. Casos de éxito se tiene a: Google App Engine, SalesForce y Azure de Microsoft.

- ***Software como Servicio (SaaS – Software as a Service)***.- Es un modelo que consiste en un despliegue de software, específicamente una aplicación informática

propietaria del proveedor al que es ofrecida como un servicio. La entidad pública no gestiona servidores, sistemas operativos o temas de almacenamiento para hacer uso de la aplicación. Todos los recursos computacionales e infraestructura necesaria donde se despliega la aplicación es propiedad del proveedor, evitando que el cliente adquiera e implemente software o hardware y realice procesos de mantenimiento y actualización. Los parámetros de seguridad son controlados por el proveedor de servicio. En este tipo de servicio el costo está basado en el uso bajo demanda y no en el número de usuarios. Una aplicación SaaS puede ser accesible a través de la Internet, independizando a los usuarios de la ubicación física, y aporta a la organización una mayor flexibilidad y evita el uso de tecnologías más complejas de comunicaciones como las redes privadas virtuales. Casos de éxito: SugarSync, Gmail, Hotmail, SkyDrive, Flickr,

A estas tres modalidades básicas, la Unión Internacional De Telecomunicaciones (UIT) de la cual forma parte el estado ecuatoriano añade otras dos [16]:

- ***Comunicaciones como servicio (CaaS – Communications as a Service).-*** Una categoría de servicios en la nube donde la capacidad proporcionada al usuario del servicio de Nube es usar servicios de comunicación y colaboración (voz sobre IP, mensajería instantánea, videoconferencia) en tiempo real.

- ***Red como servicio (NaaS – Network as a Service)***.- Una categoría de servicios en la Nube donde la capacidad proporcionada al usuario del servicio es utilizar servicios de transporte y conectividad y/o servicios de conectividad de red entre nubes (VPN flexible y extendido, ancho de banda bajo demanda etc.)

Desde la perspectiva de implementación o despliegue, la computación en la nube se la puede clasificar en:

- ***Nube Privada***.- Es aquella que permite el acceso a una sola entidad pública la cual puede ser administrada por si la misma organización o por un tercero. La infraestructura y los recursos computacionales son propios de la entidad y pueden estar alojados en su propio perímetro (Nube privada In-Situ) o en las instalaciones de un proveedor como una Nube Privada Externa o Housing. El beneficio principal es que representa un riesgo mínimo para la entidad, ya que posee control total sobre sus sistemas de información, sin embargo, el principal inconveniente es que no proporciona la escalabilidad y agilidad de una nube pública.

- ***Nube Comunitaria***.- Esquema de computación en la nube que puede ser compartida por varias organizaciones, que comparten una misión o interés común. Puede ser administrada por la misma organización o por un tercero, y puede residir dentro o fuera de las instalaciones. Al igual que la computación en la nube privada los datos pueden estar almacenados con los datos de los competidores.

- ***Nube Pública.-*** La infraestructura y los recursos computacionales se encuentran disponibles para el público en general a través de la red pública de Internet, mismas que son administradas por un proveedor y son compartidas por varios clientes. Esto es adecuado si el cliente no tiene inconvenientes al compartir espacio con otros usuarios. Casos de éxito se tiene a: IMB Smart Cloud, SunCloud, Google AppEngine, Amazon Elastic Compute Cloud (Amazon EC2), Microsoft Windows Azure, entre otros.

- ***Nube Híbrida.-*** Este tipo de infraestructura corresponde a una fusión de los dos modelos anteriormente mencionados. Esto se traduce en un nuevo modelo en el que la organización es propietaria de cierta parte (áreas en las cuáles se maneje información sensible y confidencial) y aprovecha los servicios ofertados por una Nube pública en aquellas áreas donde pueda resultar más adecuado. Posiblemente este modelo sea uno de los más utilizados en adelante por las entidades públicas ecuatorianas, quienes no quieren poner en riesgo el tema de la Seguridad del Estado.

Según la Cloud Security Alliance, la NIST [1] e ISACA, se identifican cinco características esenciales que definen a la computación en la nube:

- ***Auto servicio bajo demanda.-*** La entidad pública podría utilizar los recursos cuando considere necesario, ampliando o disminuyendo el tamaño de acuerdo a sus requerimientos momentáneos, sin precisar la interacción humana con el proveedor de servicios.

- ***Amplio acceso a través de redes***.- Disponibilidad de los recursos de red para acceder desde cualquier dispositivo, sea un computador, un teléfono móvil o una Tablet, mediante el uso de mecanismos estandarizados.

- ***Agregación y compartición de recursos***: Debido a la variación del uso de recursos computacionales, se plantea la opción de que se lo haga agrupando

múltiples entidades y que éstos puedan ajustarse en base a la demanda de los mismos, evitando así el desperdicio.

- ***Escalabilidad o adaptación inmediata***: Los recursos ofrecidos por el proveedor deben adaptarse a los requerimientos de la entidad, por ejemplo, las capacidades solicitadas deberían ser rápida y dinámicamente aprovisionadas, en algunos casos hasta de forma automática, dando la percepción al usuario que el proveedor tiene recursos ilimitados y están siempre disponibles.

- ***Servicio a la medida***: Los sistemas de Cloud Computing controlan y optimizan automáticamente el uso de los recursos, aprovechando la capacidad de medición que hace posible que los mismos puedan ser monitoreados, controlados y emitan informes, lo que brinda transparencia del servicio ante el proveedor y el usuario.

Características que según la ENISA debe incorporase las siguientes, a fin de satisfacer los requerimientos de las entidades gubernamentales [15]:

- Independientemente del tipo de implementación (privada, pública o comunitaria), los servicios de gobierno electrónico deben ser administrados y supervisados localmente o de forma centralizada por el organismo público.

- Debe proporcionar un conjunto de servicios de gobierno electrónico reutilizables para la administración pública, ciudadanía y empresas privadas.

- Independientemente de ser propietaria y administrada por terceros u organismos externos, el gobierno central o sus entidades tienen la última palabra.

- Debe proveer un modelo de negocio al servicio de los ciudadanos que permita operar la infraestructura, la plataforma y los servicios de manera tal que garantice la eficiencia y la economía de escala.

- Independientemente del modelo de servicio (infraestructura, plataforma o servicio), debe acoplarse a la legislación local, en lo concerniente a la privacidad, seguridad y resiliencia de la información.

Por lo expuesto, se evidencia que los beneficios y riesgos relacionados con la Computación en la Nube en las entidades públicas ecuatorianas dependerán en gran medida de modelo de servicio y del modelo de despliegue escogido.

1.1.3 VENTAJAS

Una de las claves para una exitosa adopción de computación en la nube por parte de las entidades públicas es comprender los beneficios o ventajas que conlleva este nuevo paradigma tecnológico, a fin de determinar los potenciales riesgos y las posibles soluciones qué deberían optar las organizaciones. Para ISACA [18] la computación en la nube posee los siguientes beneficios:

- ***Agilidad y/o inmediatez***.- Las organizaciones deben comprenden que los mercados se mueven rápidamente a la velocidad de Internet y que ser los primeros en lanzar productos comercialmente constituye una enorme ventaja. La capacidad de implementar tecnologías, desarrollar soluciones innovadoras de sistemas y satisfacer las necesidades de los clientes se ha convertido en una característica decisiva para maximizar las inversiones y oportunidades de mercado, solamente alcanzable mediante la adopción de la computación en la nube

- ***Contención de costos.-*** La computación en la nube ofrece a las organizaciones la posibilidad de utilizar recursos financieros con máxima eficiencia, que a diferencia de las soluciones tecnológicas tradicionales los costos son de índole operacional y no de inversión de capital. Debido a su la naturaleza bajo demanda, los requerimientos de infraestructura, plataforma o servicio de software requerido por la organización en periodos de mayor actividad o consumo ya no constituyen un problema y siempre serán satisfechas a corto, medio o largo plazo. Aprovechar la nube para cubrir los requisitos de capacidad y equilibrar el uso entre plataformas reduce la inversión de capital necesario y permite disponer de fondos para oportunidades operacionales e inversiones de alto retorno.

- ***Arquitectura común multiempresa (multitenancy) y/o disponibilidad***.- La naturaleza compartida de la computación en la nube permite distribuir los costos y las capacidades entre una mayor cantidad de entidades, usuarios o suscriptores; no solamente a nivel de aplicaciones e infraestructuras, sino también los conocimientos especializados de las personas que trabajan con las tecnologías, lo que permite a los proveedores abordar inversiones en soluciones de máximo nivel, no solo más económicas, sino también más eficaces, eficientes, seguras y resistentes.

- ***Confiabilidad, eficiencia y/o resiliencia***: Las características esenciales de la computación en la nube, incluido el acceso a un conjunto (pool) de recursos

compartidos a través de redes de banda ancha y una rápida flexibilidad basada en las necesidades, hacen que las soluciones en la nube sean más confiables, gracias a la incorporación de grandes fabricantes internacionales, quienes están en capacidad de suministrar una amplia gama de soluciones que satisfaga las requerimientos de las organizaciones. La sofisticación técnica de la arquitectura en la nube tal como la implementan los proveedores, la dispersión geográfica de la nube, la duplicación de datos y aplicaciones entre ubicaciones y la capacidad de conmutar instantáneamente almacenes de datos y aplicaciones a otros servidores a través de múltiples ubicaciones pueden crear una solución sumamente resistente a las caídas del sistema y las interrupciones del servicio.

- ***Escalabilidad***: Como se ha visto, la computación en la nube tiene la capacidad para atender las necesidades de la pequeña y mediana empresa, de los gobiernos y corporaciones, por tanto, cada organización puede determinar sus propias necesidades y encontrar una solución que le aporte beneficios. Para ejemplo, se puede incorporar aquellas entidades públicas con asignaciones presupuestarias limitadas que han comenzado a operar recientemente, por otro lado, para aquellas entidades con asignaciones presupuestaria holgadas, tan solo podrían necesitar complementar las capacidades existentes y cubrir necesidades especiales.

Más allá de las ventajas económica, técnica y arquitectónica que las soluciones de nube pueden proveer a las entidades de la administración pública, se evidencia la necesidad de identificar y analizarla las ventajas en términos de seguridad [19], que hagan de la Nube la solución más viable y segura:

- ***La seguridad y las ventajas de la escala***.- Todos los tipos de medidas de seguridad son más baratos cuando se aplican a gran escala. Por lo tanto, la misma cantidad de inversión en seguridad puede obtener una mejor protección. Aquí quedan incluidas las distintas medidas defensivas, como el filtrado, la administración de parches, el refuerzo de máquinas virtuales e hipervisores, los recursos humanos y su gestión y control, la redundancia de hardware y software, los sistemas de autenticación seguros, un control eficaz basado en funciones y soluciones federadas de gestión de la identidad por defecto, que también mejora los efectos de red de la colaboración de varios socios implicados en la defensa. Otras ventajas de la escala son: Ubicaciones múltiples (replicación de contenido), Redes de proximidad, Mejora del tiempo de respuesta a los incidentes y la Gestión

de amenazas, que en conjunto hacen de la computación en la nube una solución segura para cualquier tipo de organización.

- ***La seguridad como elemento diferenciador de mercado***.- La seguridad constituye una prioridad para muchos usuarios de la nube, quienes toman las decisiones relativas a la adquisición basándose en el renombre del proveedor en cuanto a confidencialidad, integridad y resistencia a los fallos, así como en los servicios de seguridad ofrecidos por el proveedor.

- ***Interfaces normalizadas para servicios de seguridad gestionados***.- Los grandes proveedores en nube pueden ofrecer una interfaz abierta y estandarizada a los proveedores de servicios de seguridad gestionados que ofrecen servicios a todos sus clientes. Potencialmente, ello genera un mercado más abierto y disponible de servicios de seguridad, donde los clientes pueden cambiar de proveedor con mayor facilidad e incurriendo en menores gastos de configuración.

- ***Escalada rápida e inteligente de recursos.-*** La capacidad de escalar dinámicamente los recursos defensivos bajo demanda posee ventajas evidentes con respecto a la resistencia a los fallos. Además, cuanto mayor sea la escalada de los distintos tipos de recursos individuales de manera granular —sin escalar la totalidad de los recursos del sistema—, más barato será responder a los picos repentinos (no maliciosos) de la demanda.

- ***Auditoría y recogida de pruebas.-*** Con el almacenamiento a libre disposición, es posible crear clones múltiples y poner en paralelo actividades de análisis y así reducir el tiempo dedicado a la investigación, lo que aporta un almacenamiento de registros más rentable a la vez que permite una actividad de registro más amplia sin afectar al rendimiento. El almacenamiento en nube de pago por uso aporta transparencia a sus gastos de almacenamiento de auditoría y facilita el proceso de ajuste a los requisitos futuros de los registros de auditoría. De este modo se incrementa la eficacia del proceso de identificación de incidentes de seguridad a medida que se producen.

- ***Actualizaciones y opciones por defecto más puntuales, efectivas y eficaces.-*** Las actualizaciones pueden aplicarse con mucha más rapidez que en los sistemas tradiciones de los clientes, que se apoyan en el modelo de parches. Para entornos

PaaS y SaaS, las aplicaciones empresariales son actualizadas periódicamente y parcheadas de manera centralizada, minimizando la ventana de vulnerabilidad.

- ***La auditoría y los acuerdos de nivel de servicio obligan a gestionar mejor el riesgo.-*** La necesidad de cuantificar las sanciones de los distintos escenarios de riesgo en los Acuerdos de Nivel de Servicio (SLA's) y la posible repercusión de los incumplimientos de la seguridad sobre el renombre, motivan una auditoría interna y unos procedimientos de evaluación del riesgo más minuciosos que los que se llevarían a cabo en condiciones normales. La frecuencia de las auditorías impuestas a los proveedores en nube tiende a exponer los riesgos que, de otro modo, no habrían sido identificados.

- ***Beneficios de la concentración de recursos.-*** Aunque sin duda la concentración de recursos tiene desventajas para la seguridad, posee el beneficio evidente de abaratar la perimetrización y el control de accesos físicos y permite una aplicación más sencilla y económica de una política de seguridad exhaustiva y un control sobre la gestión de datos, la administración de parches, la gestión de incidentes y los procesos de mantenimiento.

Una organización que tiene claro las características esenciales, los valores y beneficios provistos por la computación en la nube podrá identificar, gestionar y mitigar de manera efectiva los potenciales riesgos, a fin de establecer un gobierno y una gestión eficaz de las soluciones de Nube.

1.1.4 DESVENTAJAS

Las diferencias sutiles que presenta la computación en la nube tienen consecuencias que difícilmente se advierten de inmediato, que de acuerdo al informe "Beneficios, riesgos y recomendaciones para la seguridad de la información" de la ENISA [19] generan las siguientes desventajas o puntos de tensión:

- ***Rapidez y agilidad.-*** El factor de la rapidez para operar en el mercado, en términos de adquisición y adopción de tecnología, hace que la computación en la nube sea una estrategia adecuada para las organizaciones que anhelan aprovechar la ventaja de ser "la primera en actuar". Sin embargo, a falta de un cambio acorde en la cultura, los procesos y los procedimientos organizacionales, y sin una integración eficaz de los factores humanos a todo nivel organizacional con los servicios adquiridos pueden generar las siguientes desventajas:

- Priorización desproporcionada del valor sobre la confianza en la elección de soluciones tecnológicas.
- Pérdida de oportunidades por no considerar otras alternativas.
- Problemas en las recuperaciones por no explorar en su totalidad las opciones alternativas.
- Aumento de los costos a largo plazo por confiar en múltiples soluciones de corta duración.
- Disminución del rendimiento cuando las organizaciones dudan en introducir nuevas soluciones debido a las inversiones realizadas en las tecnologías existentes.

- ***Modificación de los límites.-*** A medida que las organizaciones confían en la tecnología para llegar a los mercados, la barrera que separa a la organización de su entorno externo desaparece. La externalización y la confianza en terceras partes para suministrar servicios tecnológicos o consolidar la estrategia organizacional socavan aún más esta barrera, ya que los roles y responsabilidades establecidas pueden modificarse abruptamente para ser transferidas hacia las líneas de negocio dejando al margen a los responsables de los procesos de gobierno y de TI. Por tanto los contratos y los acuerdos de nivel de servicio (service level agreements, SLA) pretenden asignar responsabilidades al proveedor de servicios, pero la normativa local exige que las propias entidades públicas sigan siendo los responsables. Al modificarse los límites de la organización, así como los roles y las responsabilidades a nivel interno y externo, las organizaciones pueden verse comprometida por las siguientes desventajas o factores de riesgo:
  - Confusión de roles cuando las responsabilidades (accountability) no están definidas claramente.
  - Disminución de la eficacia cuando se toman decisiones sin abordar ampliamente una ponderación entre confianza y valor antes de adquirir una plataforma, una infraestructura o un servicio de software en la nube.
  - Incapacidad para satisfacer las expectativas de los miembros y usuarios finales en materia de protección y privacidad.

- Demoras en los proyectos y costos más elevados por la necesidad de que el personal con responsabilidades de gobierno vuelva a evaluar los planes sobre la nube.
- Falta de claridad en las especificaciones de las responsabilidades (accountability) de los proveedores en los acuerdos de nivel de servicio (SLA).
- Suministro de información incompleta a los miembros de la junta directiva y a la alta dirección.

- ***Nuevas tecnologías y expectativas sobre tecnología***.- La computación en la nube ha sido definida como una tecnología rupturista, como resultado de la convergencia de la tecnología informática, las capacidades de comunicación, los enfoques aplicados al desarrollo de aplicaciones y el impacto de esos enfoques sobre el uso de la tecnología en los negocios. La introducción de nuevas tecnologías puede afectar negativamente en las organizaciones que han evolucionado su estructura para alojar soluciones suministradas y gestionadas a nivel interno. Cuando la estrategia y la arquitectura organizacional no tienen en cuenta las cualidades particulares de la computación en la nube los procesos y los procedimientos empleados por la organización pueden no adaptarse fácilmente a los cambios introducidos por la nube ocasionando la siguientes factores de riesgo siguientes:
  - Pérdida de oportunidades para extraer valor de la integración entre la nube y los sistemas de información internos.
  - Mayor vulnerabilidad debido a las incompatibilidades e inconsistencias existentes entre las soluciones en la nube y los sistemas de información internos.
  - Resultados menores de los esperados cuando no se tienen en cuenta los factores humanos en el diseño y la integración de los servicios y las infraestructuras en la nube.
  - Niveles de rendimiento organizacional que no cumplen con las expectativas porque las soluciones en la nube no respaldan plenamente los procesos organizacionales.

- Niveles de rendimiento técnico que no cumplen con las expectativas porque los procesos no aprovechan al máximo las capacidades de la tecnología en la nube.

- ***Igualdad de condiciones.-*** La computación en la nube elimina la ventaja que tradicionalmente han tenido las grandes organizaciones en términos de disponibilidad de infraestructura y especialistas de TI, ya que la pequeña y mediana empresa o entidades públicas con recursos limitados pueden recurrir a proveedores de Nube para cubrir sus necesidades tecnológicas y estar condiciones de construir su propia infraestructura que les permita ingresar en el mercado global. Para ejemplo, se tienen a pequeñas entidades aprovechando de CRM´s y Business Analytics mediante soluciones SaaS y que tradicionalmente solo disponible para las grandes organizaciones. Sin embargo, esta igualdad de oportunidades puede afectar negativamente en aquellas organizaciones que no reconocen el impacto que puede tener la Nube cuando desarrollen e implementen sus estrategias, de la siguiente forma:

  - Aparición de nuevos actores dispuestos a competir por un segmento del mercado que tradicionalmente dominaba la organización.

  - Estrategias que no tienen en cuenta las capacidades de la competencia.

  - Beneficios menores de los esperados desde las soluciones dependientes de la tecnología.

- ***Servicios de utilidad y cadenas de suministro de los servicios***.- Tradicionalmente, las organizaciones han concedido valor a ser propietarios de la tecnología y los sistemas, valor que puede verse reducido en un mercado en el que es posible adquirir, expandir o contraer al instante la tecnología y los sistemas en base a las necesidades, además, donde los costos de desarrollo y gestión se distribuyen entre una amplia base de usuarios y donde el costo está asociado directamente con los recursos utilizados. En un entorno en que la computación es una utilidad tecnológica, no se presta demasiada atención a la manera en que la infraestructura, las plataformas o los servicios de software están desarrollados. Se presta más atención a las necesidades organizacionales, los beneficios esperados que deben proporcionar y el valor que la utilidad informática puede aportar. Una organización ágil aprovecha los beneficios de las soluciones que pueden ser

utilizadas cuando se las necesita y desechadas cuando ya no aportan valor. Esas organizaciones están atentas a las oportunidades del mercado, sacan provecho de las infraestructuras de suministro, las plataformas y los servicios de software, y crean una cadena de suministro de valor que puede ser reconfigurada a medida que cambian las necesidades y condiciones del mercado. La perspectiva de que la computación es una utilidad y que la distribución de soluciones en la nube constituye una cadena de suministro de soluciones de sistemas de información genera mayor tensión sobre las organizaciones que poseen una cultura incapaz de aceptar las soluciones de utilidad, una estructura que no facilita la planificación cooperativa y procesos que no pueden aprovechar las soluciones de computación proporcionadas como una cadena de suministro de utilidades. Las organizaciones que no tienen en cuenta los efectos de las soluciones en la nube, percibidas como una utilidad informática integrada en una cadena de suministro de capacidades de TI, podrían experimentar áreas de tensión, derivando en los factores de riesgo siguientes:

- Excesiva inversión en recursos para la planificación y creación de soluciones de sistemas de información desarrollados a nivel interno.
- Resultados menores que los considerados óptimos cuando las utilidades en la nube que aportan valor quedan excluidas de la solución total.
- Duplicación de esfuerzos cuando los servicios especializados, disponibles a través de los proveedores de computación en la nube no están integrados como parte de la gestión del sistema.
- Resultados menores de los esperados cuando los componentes de utilidad no están integrados en la cadena de suministro de capacidades del sistema de información ni se los gestiona como tales.

La naturaleza técnica de la computación en la nube, su distribución e implementación, y los beneficios que promete, pueden generar áreas de tensión o desventajas para las organizaciones e entidades del sector público, dando lugar a ineficiencias en el uso de las soluciones en la nube, tanto a nivel interno como externo. En casos más extremos dichas desventajas podrían generar riesgos operacionales e incidentes que pueden tener consecuencias más significativas, por tanto, para obtener valor de la computación en la nube no basta con confiar en las

infraestructuras, las plataformas y los servicios de software en la nube, éstas deben ser integradas con las estrategias y soluciones tecnológicas que se suministran a nivel interno y con la normativa local vigente y demás normas y mejores prácticas en temas de gestión de la seguridad y gestión de riesgos. El valor, la seguridad y la confianza, así como la eficacia y la eficiencia, pueden ser obtenidos cuando las soluciones en la nube están incluidas en las estructuras de gobierno y gestión organizacional, y la gestión se ajuste a los principios rectores de la computación en la nube.

1.1.5 SITUACIÓN ACTUAL

Numerosos estudios por parte de los líderes del sector analizan la situación actual de la computación en la nube a nivel mundial y desde diferentes puntos de vista. Por ejemplo, la Business Software Alliance ha publicado un estudio sobre 24 países [20]. En él se puntúa a los países a partir de un índice de siete áreas:

- Protección de la privacidad
- Seguridad de la información.
- Medidas contra los ciberdelitos.
- Protección de la propiedad intelectual.
- Portabilidad de los datos
- Liberalización de las normas comerciales.
- Infraestructuras de tecnologías de la información.

El estudio establece una clara diferencia entre las economías avanzadas (encabezadas por Japón) y los países en desarrollo. Además, se indica que entre los elementos que obstaculizan la adopción de la nube destacan los siguientes:

- Insuficientes avances en la implantación de una red de banda ancha, ya sea a nivel institucional, nacional e internacional.
- Políticas restrictivas sobre el contenido de Internet, caso particular y último China en contra de google [21].

- Trato discriminatorio a las empresas extranjeras de tecnología.
- Falta de un marco adecuado para el desarrollo de normas de TIC.

A continuación, se realiza una breve síntesis por región de la situación actual de la computación en la nube, basada en publicaciones de importantes organismos que impulsan la adopción de la computación en la nube:

- ***UNIÓN EUROPEA.-*** Mediante el comunicado "Liberar el potencial de la computación en nube en Europa" [14], la Comisión Europea adoptó la Estrategia Europea de Cloud Computing a fin de habilitar y facilitar la adopción de las tecnologías de computación en la nube en todos los sectores de la economía como palanca de productividad, crecimiento y empleo. Estrategia que juega un papel fundamental para el impulso y adopción del nuevo modelo de servicios TI por parte del sector público, además, se proponen medidas para obtener 2,5 millones de nuevos puestos de trabajo en Europa, así como un incremento anual del PIB en la Unión Europea igual a 160.000 millones de euros (en torno a un 1 %) de aquí a 2020.

  Además en el comunicado se ofrece 10 recomendaciones básicas para una implementación segura y exitosa de los servicios de nube gubernamental, cuyo uso se recomienda como el más económico y seguro para la protección de los datos de los ciudadanos. Estas recomendaciones son [15]:

  - Apoyar el desarrollo de una estrategia europea en materia de nubes gubernamentales.
  - Desarrollar un modelo empresarial que garantice la sostenibilidad y las economías de escala para soluciones de nube gubernamental.
  - Fomentar la definición de un marco regulador que trate el «problema de la localidad».
  - Fomentar la definición de un marco de trabajo que atenúe el problema de la «pérdida de control».
  - Desarrollar un marco común de Acuerdos de Nivel de Servicio (SLA, por sus siglas en inglés).

- Optimizar el cumplimiento de las normativas específicas de cada país y de la UE con relación a las soluciones de nube.
- Desarrollar un marco de certificación.
- Desarrollar un conjunto de medidas de seguridad para todos los modelos de implementación.
- Apoyar las investigaciones y los estudios académicos relacionados con la computación en nube.
- Desarrollar disposiciones para mejorar la privacidad.

- ***ASIA.***- El índice elaborado para Asia evalúa diez características fundamentales de 14 países, como la conectividad internacional, la calidad de la red eléctrica, la eficacia empresarial y el riesgo global (como la presencia de fallas sísmicas). El estudio concluye que Japón lidera la región, seguido de cerca por Hong Kong (China), la República de Corea y Singapur. Por su conectividad internacional y sus numerosos centros de datos, Hong Kong tiene potencial para convertirse en un importante centro de datos en el norte de Asia. La República de Corea se ha dotado de una ambiciosa estrategia sobre la nube que recibirá una financiación pública de hasta 2.000 millones de USD para el 2014.

- ***ÁFRICA.-*** Un estudio realizado por la UTI en África, indica que esta región emplea un índice de preparación ante la nube basado en factores como la penetración de Internet, la tasa de alfabetización y la pérdida de valor consecuencia de los apagones eléctricos, que ubican a Sudáfrica como el país mejor puntuado de esta región, seguido por Zimbabwe, Sudán, Senegal y Kenya. De igual forma este estudio recomienda las siguientes medidas para facilitar la computación en nube:
  - Avanzar en materia de regulación para abordar las preocupaciones sobre protección de datos y seguridad;
  - Garantizar que los países estén al tanto de las mejores prácticas en materia de regulación;
  - Preparar meticulosamente los contratos de externalización de la computación en nube, incluyendo cláusulas sólidas sobre disponibilidad y seguridad de los datos;
  - Garantizar que dichos contratos reflejen los requisitos reguladores;

- Crear centros de datos en África para reducir el coste del ancho de banda y aumentar la velocidad de acceso;
- Velar por que los centros de datos se preocupen por los servicios, sean rápidos y ecológicos y estén automatizados y bien protegidos;
- Introducir o mejorar la regulación, como las leyes de protección de datos;
- Asegurar la normalización y la regulación transfronterizas participando en iniciativas de normalización de la nube.

- ***AMÉRICA LATINA***.- Durante el seminario "Promoviendo La Computación En La Nube En Europa Y América Latina" realizado el 4 de febrero de 2014, en Santiago de Chile, se abordaron mediante un taller los impactos y desafíos de la computación en la nube en Europa y América Latina, en la que participaron miembros de la Comisión Económica para América Latina y el Caribe (CEPAL), la Comisión Europea, la Fundación País Digital, la CAF, la Subsecretaría de Telecomunicaciones de Chile, la Fundación País Digital y la Cámara de Comercio de Santiago.

  En dicho evento se pudo evidenciar que la computación en la nube en América Latina puede suponer un medio importante para reducir la desigualdad y la brecha con otras regiones, al reducir la barrera de acceso a recursos tecnológicos que antes eran impagables, lo cual se ve plasmado en la rapidez de adopción en el resto del mundo, lo que podría implicar una oportunidad para la región para generar y exportar tecnología. De dicho taller también se puede destacar lo siguiente:

  - Para la CEPAL, la computación en la nube es fundamental para reducir la desigualdad, consecuentemente con esta opinión durante la celebración del seminario Promoviendo la computación en la nube en Europa y América Latina (febrero 2014) anunció la creación de un Foro Inter-Regional (UE-LA) permanente de intercambio de experiencias, debate y formulación de políticas para aprovechar sinergias entre los esfuerzos europeos y latinoamericanos tendientes a fomentar la masificación de la computación en la nube. En él se prestará especial atención a la armonización de estándares y la seguridad y portabilidad de datos, así como a un tema de creciente actualidad: la privacidad de los datos personales y empresariales.
  - Para la Asociación Iberoamericana de Centros de Investigación y Empresas de Telecomunicaciones (AHCIET), la computación en la nube supone uno

de los retos a enfrentar en el futuro cercano. El objetivo es coadyuvar al desarrollo de tales servicios en la región mediante el dialogo público privado tendiente a crear una visión regional que ayude a forjar un clima de seguridad y certidumbre para los usuarios.

- A nivel de operadores en América Latina son ya varios los operadores (América Móvil (Telmex), AT&T, Telefónica, Verizon (Terremark) y KIO México) que ofrecen servicios de almacenamiento y gestión empresarial en la Nube, como: SAP Business One en la nube, que integra gestión financiera, compras, ventas, distribución, gestión de atención al cliente y gestión de inventarios.

- ***ECUADOR.-*** Según la normativa legal vigente [6] el gobierno ecuatoriano "prohíbe expresamente a las entidades de la Administración Pública la contratación, acceso y uso de servicios de correo electrónico en la Internet (Nube), para uso institucional o de servidores públicos, con empresas privadas o públicas cuyos centros de datos, redes (salvo la Internet), equipos, software base y de gestión de correo electrónico y cualquier elemento tecnológico necesario, se encuentren fuera del territorio nacional; y adicionalmente, si las condiciones de los servicios que tales empresas prestaren no se someten a la Constitución y Leyes Ecuatorianas", sin embargo, iniciativas como la "Implementación del Centro Nacional de Datos de Ecuador" [22] hacen prever una pronta adopción de la computación de la nube por parte de las entidades de la Administración Publica Ecuatoriana semejante a su similares de la región como Brasil, Argentina y Chile. De acuerdo a la "Guía para el análisis de factibilidad en la implantación de tecnologías de cloud computing en empresas del Ecuador" [23] se evidencia que primero crece más la oferta de estos servicios que la demanda en sí, para ejemplo se tiene a empresas ecuatorianas como CNT S.A., Telconet, EIKON S.A., Econocompu S.A., o CloudConsulting que ofrecen servicios a nivel empresarial, gubernamental y social. Otros ejemplos de operadores internacionales que apuestan por la computación en la nube en Ecuador están la empresa Telconet, que inauguró dos centros de datos de alta disponibilidad más grandes del país y de Latinoamérica con categoría TIER III y IV para ofrecer a sus clientes servicios IaaS; Cloud Ecuador, quienes ofrecen los tres modelos de despliegue IaaS, PaaS y SaaS y Telefónica Ecuador, también pone a disposición centros de datos, pero con localización en otros países como Brasil, Argentina o

Estados Unidos enfocados hacia el uso de empresas multinacionales que tienen sucursales en Ecuador.

Según la matriz FODA planteada en el “Análisis De Los Riesgos Técnicos Y Legales De La Seguridad En Cloud Computing” [24], se evidencia que la adopción de servicios en la Nube en Ecuador es viable, ya que se confirma un terreno adecuado para su despliegue.

FORTALEZAS	OPORTUNIDADES
• Conceptos relativamente nuevos en la región, por lo que su expansión se debe realizar de forma controlada. • Desarrollo rápido de una infraestructura de TI. • Especialistas en el área de TI realizando el manejo de los servicios. • Escalabilidad en la infraestructura tecnológica, sin nuevas inversiones. • Colaboración con las PYMES que son potenciales clientes, economizando costos en tecnología. Las PYMEs constituyen un alto porcentaje dentro de la industria ecuatoriana.	• Permitir que las organizaciones ecuatorianas puedan alcanzar un nivel tecnológico de países desarrollados. • Centrar los esfuerzos de las organizaciones hacia el núcleo del negocio. • Reducir costos en la infraestructura de IT de las grandes entidades gubernamentales. • Permitir que las empresas cuenten con infraestructuras controladas con todos los estándares del sector. • Incremento de la seguridad en las aplicaciones.
DEBILIDADES	**AMENAZAS**
• Falta de una cultura de Seguridad de la Información, en proveedores y clientes. • Falta de conocimientos de Cloud Computing, tanto de sus beneficios como de sus debilidades. • El índice de penetración de Internet no sobrepasa el 30%, por lo que el acceso a la Nube mediante la Internet puede verse limitado.	• Pérdida de control en los datos que manejarán los proveedores. • Proveedores que no están certificados en estándares de Seguridad de la Información. • Monopolio por parte de los pocos proveedores de servicio que pueden brindar el servicio de la Nube. • Carencia de regulación para la expansión de los servicios.

• Capacidades de acceso a la Internet relativamente bajas, provocando procesos y aplicaciones lentas.

Tabla 1.1.8.1: Situación de la computación en la nube en el mercado ecuatoriano [17].

Sin embargo, la no existencia de una normativa legal que regule los servicios brindados por un proveedor de Servicios en la Nube, puede acarrear problemas en el ámbito legal entre clientes y proveedores ecuatorianos, pese a sus esfuerzos de protegerse con las leyes ecuatorianas existentes, que simplemente no contempla todas las especificaciones que las soluciones que la Nube demanda.

En este contexto, la computación en la nube en general se plantea para el gobierno ecuatoriano como solución fundamental para reducir costos en la provisión de servicios de TI a todas las entidades de la Administración Pública, bajo estrictas normas de calidad y de aseguramiento de la información. Además, según estimaciones recientes [25] para la Unión Europea, Estados Unidos y países latinoamericanos como: Argentina, Brasil Colombia y Chile, muestran que la masificación de la computación en la nube impulsaría la creación de decenas de miles de pequeñas empresas y centenares de miles de empleos.

1.2 ANÁLISIS DE GESTIÓN DE RIESGOS DE SERVICIOS DE CLOUD COMPUTING EN INSTITUCIONES GUBERNAMENTALES.

Muchos de los riesgos frecuentemente asociados a la computación en la nube no son nuevos y se pueden encontrar en las organizaciones de la actualidad. Una buena planificación de las actividades de gestión de riesgos será crucial para asegurar que la información esté tanto disponible como protegida. Los procesos y procedimientos de negocio deben dar cuenta de la seguridad, y es posible que los gerentes de seguridad de la información deban ajustar las políticas y los procedimientos de sus organizaciones para satisfacer las necesidades del negocio. Debido al ambiente dinámico de los negocios y a la atención puesta sobre la globalización, es muy reducido el número de organizaciones que no tercerizan una parte determinada de su negocio. Por lo tanto, establecer una relación con un

tercero significa que el negocio no sólo utiliza los servicios y la tecnología del proveedor de la nube, sino que también debe lidiar con la manera como el proveedor dirige su organización, la arquitectura de la que éste dispone, así como con la cultura y las políticas de la organización del proveedor, de ahí la pregunta critica que toda organización se debe plantear y que debe tener claro durante un proceso de migración o adopción de servicios de Nube es: ¿***Quien administra qué***?

De acuerdo a la Figura 1.1.8.1, dependiendo del modelo de servicio escogido el nivel de administración o responsabilidad se incrementa inversamente proporcional desde el punto de vista del cliente respecto al del proveedor de servicio, y viceversa. No siendo la excepción para los modelos de despliegue público o privado.

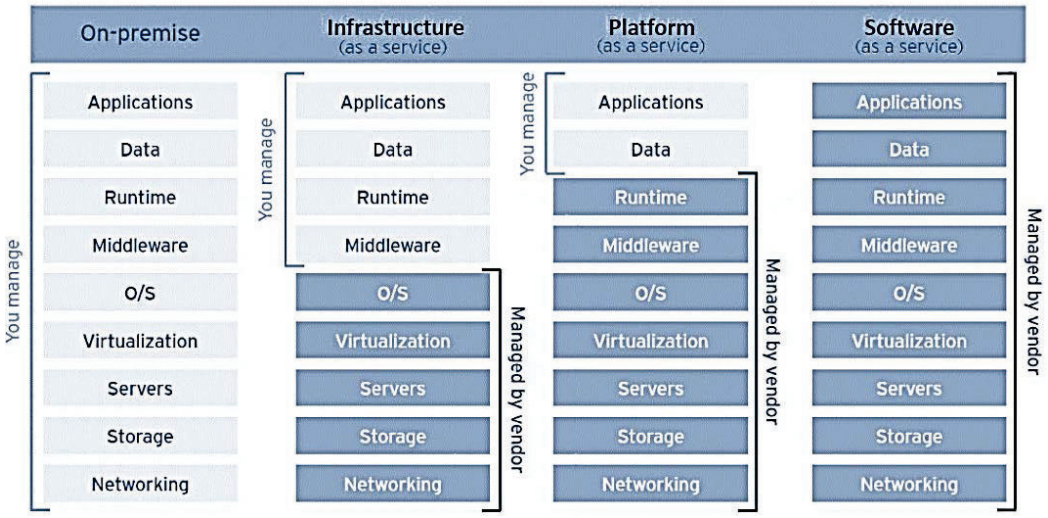

Figura 1.1.8.1 Niveles de administración de computación en la nube [26]

Para Joaquín Campos, ejecutivo de Security Systems de IBM, los últimos ataques cibernéticos de los que están siendo blanco las empresas y/o gobiernos que almacenan información confidencial en la nube se deben a una falta de políticas de seguridad, ya que según el experto "El plazo medio que una organización lleva para percibir que hay una amenaza es de 8 meses. Y para resolverla, le puede tomar hasta más de un año. El tema más importante es que la organización tenga las políticas de seguridad correctas para proteger su ambiente y que después de eso tenga las tecnologías que sean necesarias", además, "Con respecto a las políticas de regulaciones locales" señaló que son temas del gobierno, y que el proveedor tiene que comprender cuáles son las decisiones de estos y ofrecer lo que es mejor

para los servicios y la seguridad de los gobiernos como clientes" [27]. Sin embargo para el keniano Alex Gakuru director ejecutivo de Content Development Intellectual Property Trust (IP Trust-Kenia) [22], mediante la computación en la nube por primera vez se tiene una situación en la que se están utilizando las leyes extranjeras en países locales, donde el principal perjudicado es el usuario ya que nadie garantiza que las leyes del país en que reside los protegerán frente al uso y acceso indebido de su información por parte de terceros, más aún cuando la ley del país de origen del Proveedor se aplica incluso en el país extranjero en el que opera el CSP, de ahí la necesidad de contar con una normativa internacional que regule la computación en la nube, independiente de la legislación del país de origen del proveedor a fin de que los usuarios tengan el derecho de saber todo lo que se está haciendo con sus datos por parte de las corporaciones privadas.

Lamentablemente, al momento el estado ecuatoriano no cuenta con una normativa legal que regule los servicios provistos por el proveedor de servicios en la nube, como lo hace Estados Unidos de América, la Unión Europea, Canadá, Suiza y Argentina, mismos que al momento se han adherido al acuerdo de Puerto Seguro para la protección de la información.

A más de los puntos de conflictos relacionados con la computación en la nube, citados en el numeral 1.1.7, se tiene:

- Las organizaciones deben ser específicas al seleccionar un proveedor. La reputación, los antecedentes y la sostenibilidad son factores que se deben tomar en consideración. La sostenibilidad es particularmente importante para garantizar que los servicios estarán disponibles y que los datos se podrán rastrear.

- Con frecuencia, el proveedor de la nube asume la responsabilidad de manejar la información, lo cual constituye una parte crítica del negocio. No actuar de conformidad con los niveles de servicio acordados puede perjudicar no sólo la confidencialidad, sino también la disponibilidad, lo que afecta enormemente las operaciones del negocio.

- La naturaleza dinámica de la computación en la nube podría resultar confusa en cuanto a dónde reside la información realmente. Cuando se requiere la recuperación de la información, es posible que haya demoras.

- El acceso por parte de terceros a información sensitiva crea el riesgo de comprometer la confidencialidad de la información. En la computación en la nube, esto pudiera representar una amenaza significativa a la hora de asegurar la protección de la propiedad intelectual y los secretos comerciales.

- Las nubes públicas permiten desarrollar sistemas de alta disponibilidad en niveles de servicio que son imposibles de crear en redes privadas, a no ser a un costo extremadamente alto. El aspecto negativo de esta disponibilidad es que es posible mezclar los activos de información con los de otros clientes de la nube, incluso de competidores. Cumplir con las regulaciones y leyes de diferentes regiones geográficas puede ser desafiante para las organizaciones. En estos momentos, es muy limitado el precedente relacionado con la confiabilidad en la nube. Es necesario obtener asesoría legal apropiada para asegurar que el contrato especifique las áreas donde el proveedor de la red es responsable legal y financieramente por las ramificaciones resultantes de problemas potenciales.

- Debido a la naturaleza dinámica de la nube, es posible que la información no se localice inmediatamente si ocurriera un desastre. Los planes de continuidad del negocio y de recuperación en caso de desastre deben estar bien documentados y probados. El proveedor de la nube debe entender la función que desempeña en términos de copias de respaldo, respuesta y recuperación en caso de desastre. Los tiempos objetivos de recuperación deben estar especificados en el contrato.

A continuación se analizan las amenazas, vulnerabilidades y riesgos descritos por los líderes del sector de Cloud Computing.

1.2.1 AMENAZAS

De acuerdo al informe “Top Threats to Cloud Computing V1.0 [28]” publicado por Cloud Security Alliance se identifican las siguientes mayores amenazas para una infraestructura de Nube, misma que se actualizan regularmente en consenso de los expertos y que sirven como guía a las organizaciones en la toma de decisiones y en la adopción de estrategias que involucran Cloud Computing:

- ***A1 - Abuso y mal uso del cloud computing***.- Amenaza que afecta principalmente a los modelos de servicio IaaS y PaaS y se relaciona con un registro de acceso a estas infraestructuras o plataformas poco restrictivo.

- ***A2 - Interfaces y API poco seguros***.- Amenazas relacionadas con las interfaces y API proporcionadas por el proveedores para controlar, provisionar, monitorizar e interactuar con todos los recursos.

- ***A3 - Amenaza interna***.- Relacionado con incidentes de seguridad provocados por empleados descontentos o accidentes por error o desconocimiento. A esto se suma la falta de procedimientos para la baja y alta de usuarios con acceso a la infraestructura de nube.

- ***A4 - Problemas derivados de las tecnologías compartidas.-*** Amenaza que afecta a los modelos IaaS, ya que los componentes físicos no fueron diseñados para una arquitectura distribuida o compartida.

- ***A5 - Pérdida o fuga de información***.- Amenaza relacionada con el comprometimiento de información crítica debido al elevado número de interacciones que se da en la arquitectura de la nube.

- ***A6 - Secuestro de sesión o servicio***.- Amenaza relacionada con la obtención de credenciales de un usuario con acceso al entorno por parte de un atacante acceder a actividades y transacciones, manipular datos, devolver información falsificada o redirigir a los clientes a sitios maliciosos.

- ***A7 - Riesgos por desconocimiento***.- Amenazas relacionadas el deterioro de la seguridad por falta de conocimiento de la infraestructura de Cloud Computing, a esto se suma, la reducción de la cantidad de software y hardware de seguridad.

- ***A8 - Transmisión de datos vulnerable***.- Amenaza relacionada con la falta de mecanismos básicos como la encriptación (SSL/TSL) o cifrado durante el proceso de transferencia de datos hacia la nube, ya que pueden ser interceptados por atacantes man-in-the-middle.

- ***A9 - Perfil de riesgo desconocido:*** Amenaza relacionada con la falta de una línea base del perfil de riesgo de los sistemas e infraestructura por parte de la organización previo a la adopción de la computación en la nube.

Amenazas que dependiendo del tipo de modelo de servicio de computación en la nube, pueden ser aprovechadas ocasionando un gran impacto en el servicio o datos.

1.2.2 VULNERABILIDADES Y RIESGOS

Según el informe “Beneficios, riesgos y recomendaciones para la seguridad de la información” [19], publicado por la ENISA, se identifican 35 riesgos y 44 vulnerabilidades, mismas que se encuentran categorizadas en cuatro grupos y relacionadas entre sí de acuerdo a la Tabla 1.2.2.1.

De acuerdo a dicho informe los potenciales riegos que toda organización debe tener presente al momento de migrar o adoptar la computación en la nube son aquellos calificados con un alto nivel de riesgo.

CATEGORÍA	RIESGO	VULNERABILIDAD	NIVEL
C01 – Políticos y organizativos	R01 - Vinculación	V01, V02, V03, V04	ALTO
C01 – Políticos y organizativos	R02 - Pérdida de gobernanza	V01, V04, V05, V06, V07, V08, V09, V10, V11, V12, V13, V14, V15	ALTO
C01 – Políticos y organizativos	R03 - Desafíos de cumplimiento	V01, V04, V09, V11, V14, V15	ALTO
C01 – Políticos y organizativos	R04 - Pérdida del renombre empresarial a raíz de actividades de prestación conjunta	V16, V17, V18	MEDIO
C01 – Políticos y organizativos	R05 - Error o cancelación del servicio en nube	V02, V03, V04	MEDIO
C01 – Políticos y organizativos	R06 - Adquisición del proveedor en nube	V04	MEDIO
C01 – Políticos y organizativos	R07 - Fallo en la cadena de suministro	V02, V03, V04, V10	LEVE
C02 – Técnicos	R08 - Agotamiento de recursos (prestación excesiva o insuficiente)	V03, V19, V20, V21	MEDIO
C02 – Técnicos	R09 - Fallo de aislamiento	V16, V17, V18, V22, V23	ALTO
C02 – Técnicos	R10 - Miembros maliciosos de proveedores en nube. Abuso de funciones privilegiadas	V05, V06, V24, V25, V26, V27, V28, V29	ALTO
C02 – Técnicos	R11 - Compromiso de interfaz de gestión (manipulación, disponibilidad de la infraestructura)	V25, V26, V29, V30, V31	MEDIO
C02 – Técnicos	R12 - Interceptación de datos en tránsito	V04, V22, V23, V25, V32, V33	MEDIO
C02 – Técnicos	R13 - Fuga de datos durante la carga/descarga dentro de la nube	V04, V22, V23, V25, V32, V33	MEDIO
C02 – Técnicos	R14 - Supresión de datos insegura o ineficaz	V34	MEDIO
C02 – Técnicos	R15 - Distribución de denegación de servicio (DDoS)	V26, V31, V35	MEDIO
C02 – Técnicos	R16 - Denegación económica de servicio (EDoS)	V21, V25, V30, V36, V37	MEDIO

C02 – Técnicos	R17 - Pérdida de las claves de codificación	V38, V39	MEDIO
C02 – Técnicos	R18 - Realización de escaneados o detecciones maliciosas	V22, V23	MEDIO
C02 – Técnicos	R19 - Motor de servicio de compromiso	V16, V18	MEDIO
C02 – Técnicos	R20 - Conflictos entre los procedimientos de refuerzo del cliente y el entorno de la nube	V04, V05	BAJO
C03 – Legales	R21 - Órdenes judiciales y descubrimiento electrónico	V11, V15, V16	ALTO
C03 – Legales	R22 - Riesgo derivado del cambio de jurisdicción	V11, V15	ALTO
C03 – Legales	R23 - Riesgos de la protección de datos	V11, V15	ALTO
C03 – Legales	R24 - Riesgos relativos a la licencia	V04	MEDIO
C04 – No específicos a la nube	R25 - Brechas en la red	V16, V26, V31	MEDIO
C04 – No específicos a la nube	R26 - Gestión de la red (congestión de la red/fallo en la conexión/uso no óptimo)	V16, V26, V31, V40	ALTO
C04 – No específicos a la nube	R27 - Modificación del tráfico de la red	V13, V32, V36, V37	MEDIO
C04 – No específicos a la nube	R28 - Escalada de privilegios	V05, V06, V18, V24, V25, V31, V36, V37	MEDIO
C04 – No específicos a la nube	R29 - Ataques de ingeniería social (suplantación)	V16, V27, V32, V36, V41	MEDIO
C04 – No específicos a la nube	R30 - Pérdida o compromiso de los registros operativos	V25, V26, V36, V37, V42, V43	BAJO
C04 – No específicos a la nube	R31 - Pérdida o compromiso de los registros de seguridad (manipulación de la investigación experta)	V25, V26, V36, V37, V42, V43, V44	BAJO
C04 – No específicos a la nube	R32 - Pérdida o robo de las copias de seguridad	V25, V27, V36, V37	MEDIO
C04 – No específicos a la nube	R33 - Acceso no autorizado a los locales (incluido el acceso físico a las máquinas y otras instalaciones)	V27	BAJO
C04 – No específicos a la nube	R34 - Robo de equipos informáticos	V27	BAJO
C04 – No específicos a la nube	R35 - Catástrofes naturales	V40	BAJO

Tabla 1.2.2.1: Análisis de riesgos según la ENISA

Toda vez que se han identificado los potenciales riesgos que conllevaría la adopción de la computación en la nube, es necesario establecer aquellos que se

encuentran relacionados con el modelo de Infraestructura como Servicio (IaaS), ya que es el modelo sobre el cual se desarrollará el presente trabajo.

De acuerdo a la Tabla 1.2.2.2, el riesgo de Pérdida de Gobernanza posee el nivel más alto de que las amenazas del numeral 1.2.1 exploten las vulnerabilidades asociadas a dicho riesgo, con la consecuente pérdida o daño a los activos o impacto al proceso de adopción del IaaS.

R02 - PÉRDIDA DE GOBERNANZA		
Probabilidad	MUY ALTA	Comparativa: Mas Alta
Impacto	MUY ALTO (depende de la organización) (IaaS MUY ALTO, SaaS Bajo)	Comparativa: Igual
Vulnerabilidad	• Aplicación deficiente de las definiciones de funciones • Aplicaciones inter-nube que crean dependencia oculta • Auditoría o certificación no disponible para los clientes • Ausencia de un acuerdo de depósito de fuentes • Cláusulas SLA con compromisos en conflicto para con diferentes partes. • Falta de control en el proceso de evaluación de vulnerabilidad • Falta de información sobre jurisdicciones • Falta de integridad y transparencia en los términos de uso Propiedad de los activos confusa • Falta de tecnologías y soluciones estándar • Falta de transparencia • Funciones y responsabilidades confusas • Sincronización de las responsabilidades o las obligaciones contractuales externas a la nube • Sistemas de certificación no adaptados a las infraestructuras de nube	
Activos Afectados	• Renombre de la compañía	

	• Confianza del cliente • Fidelidad y experiencia del empleado • Datos personales sensibles • Datos personales • Datos personales críticos. • Prestación del servicio – Servicio en tiempo real • Prestación del Servicio.
Riesgo	ALTO

Tabla 1.2.2.2: Análisis de riesgo Pérdida de Gobernanza [19]

La pérdida de gobernanza y control repercute gravemente sobre la estrategia de la organización y en su capacidad de cumplir con su misión y objetivos. Además podría generar la imposibilidad de cumplir los requisitos en materia de seguridad, confidencialidad, integridad y disponibilidad de los datos, con el consecuente deterioro del rendimiento y de la calidad del servicio, por no mencionar la introducción de desafíos de cumplimiento. A esto se suma la posibilidad de que las siguientes vulnerabilidades sean aprovechadas por un atacante:

- ***Funciones y responsabilidades confusas***.- Vulnerabilidad relacionada con la atribución inadecuada de funciones y responsabilidades en la organización del proveedor en nube.

- ***Aplicación deficiente de las definiciones de funciones.-*** Separación inadecuada de funciones por parte del proveedor que puede conducir a roles excesivamente privilegiados que pueden convertir a los sistemas muy grandes en vulnerables.

- ***Sincronización de las responsabilidades o las obligaciones contractuales externas a la nube.-*** Vulnerabilidad asociada con la inconciencia por parte del usuario de nube respecto a las responsabilidades que debe asumir. Existe la tendencia errónea de atribuir al proveedor de nube toda la responsabilidad relacionada con el aseguramiento de la información, pese a estar claramente señalado en los términos del contrato.

- ***Cláusulas SLA con compromisos en conflicto.-*** Vulnerabilidad asociada a conflictos entre cláusulas de los Acuerdos de Nivel de Servicio o en cláusulas de otros proveedores.

- ***Auditoría o certificación no disponible para los clientes.-*** El proveedor en nube no puede ofrecer ninguna garantía al cliente vía una certificación de auditoría, ya que se ha dado casos que ciertos proveedores utilizan hipervisores de código abierto que no han alcanzado certificación alguna de seguridad.

- ***Falta de tecnologías y soluciones estándar.-*** Vulnerabilidad relacionada a la falta de medios estándar lo que a la postre se traduce en atadura del cliente hacia un determinado proveedor, más aún si éste cesase sus operaciones.

- ***Almacenamiento de datos en jurisdicciones múltiples y falta de transparencia sobre este punto.-*** Vulnerabilidad asociada a la falta de información actualizada sobre la ubicación exacta (jurisdicción) de los datos espejos.

- ***Falta de control en el proceso de evaluación de vulnerabilidad.-*** Vulnerabilidad asociada con restricciones impuestas por el proveedor, tales como, el escaneado de puertos o los tests de vulnerabilidad, más aún si en los términos del contrato se hace responsable al cliente de asegurar sus elementos de infraestructura.

- ***Sistemas de certificación no adaptados a las infraestructuras de nube.-*** Dado la característica de tecnología emergente de la computación en la nube, hasta la fecha no se dispone de controles específicos, lo que quiere decir que las vulnerabilidades de seguridad probablemente pasarán desapercibidas.

- ***Falta de información sobre jurisdicciones.-*** Vulnerabilidad asociada con la falta de información de donde (jurisdicción) sus datos son almacenados y procesados, ya que pueden ser blanco fácil de confiscación debido a una entrada forzada.

En referencia a la Figura 1.1.8.1 es importante que las funciones y responsabilidades en materia de seguridad estén bien definidas y entendidas entre el cliente y proveedor, más aún para una solución IaaS que delega mayor responsabilidad al cliente. En la Tabla 1.2.2.3 se ilustra una distribución de responsabilidad típica y racional para una IaaS, que no es mandatorio. En caso de

que se apliquen condiciones estándar de servicio – que no puedan negociarse – los clientes en nube deben verificar el ámbito de sus responsabilidades.

CLIENTE	PROVEEDOR
• Mantenimiento del sistema de gestión de identidad • Gestión del sistema de gestión de identidad • Gestión de la plataforma de autenticación (incluido el cumplimiento de la política de contraseñas) • Gestión de parches del sistema operativo de invitado y procedimientos de refuerzo (también verificación de cualquier conflicto entre el procedimiento de refuerzo del cliente y la política de seguridad del proveedor) • Configuración de la plataforma de seguridad de invitado (normas del cortafuego, ajuste de IDS/IPS, etc.) • Supervisión de los sistemas de invitado • Mantenimiento de la plataforma de seguridad (cortafuegos, IDS/IPS de alojamiento, antivirus, filtrado de paquetes) • Recogida de registros y control de la seguridad.	• Infraestructura de soporte físico (instalaciones, espacio en bastidor, potencia, refrigeración, cableado, etc.) • Disponibilidad y seguridad de la infraestructura física (servidores, almacenamiento, red, ancho de banda, etc.) • Sistemas de alojamiento (hipervisor, cortafuego virtual, etc.)

Tabla 1.2.2.3: Funciones y responsabilidades IaaS

Para finalizar, la computación en la nube presenta desafíos en términos de riesgos que deben ser identificados, y puntos de tensión que es necesario evaluar. El riesgo relacionado con la computación en la nube que el personal directivo debe evaluar excede los aspectos meramente técnicos de la virtualización y las cuestiones relacionadas con la dependencia de un proveedor externo de servicios. La nube ofrece a las organizaciones ventajas competitivas resultantes de una mayor agilidad

en el desarrollo y la distribución de TI, la capacidad de contener los costos, la posibilidad de compartir recursos con otras organizaciones cliente o “inquilinos” (tenants), la confianza que las infraestructuras en la nube pueden generar y la escalabilidad de las soluciones. La necesidad de sopesar los beneficios esperados y los riesgos de orden legal, operacional o reputacionales, requiere que el personal directivo integre la gestión de riesgos en la nube con un programa de gestión de riesgos de negocio más amplio y que esté relacionado con el uso de sistemas de TI.

1.3 DISCUSIÓN DE PROBLEMAS Y POSIBLES SOLUCIONES

Los clientes de la computación en la nube Gubernamental (entidades gubernamentales, entidades privadas o sociedades y ciudadanía) necesitan que el gobierno o el que haga las veces de proveedor de servicios en la Nube Gubernamental, garanticen que aplican prácticas adecuadas en materia de seguridad (física, legal, políticas y técnicas) para mitigar los riesgos a los que se encuentran expuestos (por ejemplo, los ataques distribuidos de denegación de servicio o DDoS), requisito necesario para poder tomar decisiones de negocio correctas y mantener u obtener certificados de seguridad; de igual forma, para hacer frente al creciente incremento de solicitudes de auditoría por parte de los organismos de control nacional e internacional.

1.3.1 PROBLEMAS

Como se ha podido evidenciar en el numeral 1.2, la computación en la nube, al igual que numerosos beneficios también contempla números riesgos, que si no son gestionados adecuadamente puede generan graves problemas a la organización, más aún, si no existe una normativa internacional que la regule pese a la gran variedad de iniciativas por parte de los principales organismos de normalización internacional que continúan generando políticas para abordar y aprovechar la nube, respetando el principio general de que lo que sucede en la nube no puede quedar fuera de los controles y normas jurídicas existentes tanto a nivel local como internacional.

A continuación, se analiza ciertos problemas de la computación en la nube desde la perspectiva del usuario abordado por el informe de la UIT “Tendencias en las Reformas de las Telecomunicaciones [29]”:

- ***¿Competencia o control?***

  La hegemonía de determinados proveedores, en el caso particular de Ecuador, las empresas pública de telecomunicaciones, podría atentar contra la naturaleza competitiva del mercado de la Nube en cualquiera de sus segméntenos (SaaS, PaaS y/o IaaS) y frenar al flujo de datos, aplicaciones o servicios por el mero hecho de ser entidades públicas. Efectos anticompetitivos fruto de la falta de normas de la industria o de una norma de facto atribuible al líder del mercado.

  La concesión restrictiva de licencias también puede menoscabar la competencia. Para ejemplo se tiene a Apple, que en virtud de sus acuerdos de licencia con desarrolladores independientes, impuso el uso exclusivo de sus propias herramientas de programación y aprobó lenguajes para el desarrollo de aplicaciones para iPhone. La Comisión Europea consideró que la imposición de estas restricciones podía afectar a la competencia, y en septiembre de 2010 Apple las eliminó de forma voluntaria.

  Las prácticas de contratación pública también pueden dar pie a tendencias anticompetitivas. Para ejemplo el caso de Google contra el Departamento de Interior de Estados Unidos sobre un contrato de 59 millones de USD para servicios de TIC que supuestamente distorsionaban la competencia de manera ilícita, al exigir que las tecnologías de mensajería se basasen en Microsoft Business Productivity Online Suite, excluyendo así a Google de los concursos públicos y restringiendo la competencia. Para el caso ecuatoriano se tiene los procesos de régimen especial que favorecen a proveedores del sector público.

  Decisiones que pretenden evitar la hegemonía de un fabricante o proveedor y la debilitación de la competencia.

- ***Preocupaciones medioambientales***

  Está claro que los servicios en la nube permiten a los usuarios mejorar su eficacia en equipamiento o inmobiliario. Sin embargo, los grandes centros de datos consumen ingentes cantidades de energía, lo cual plantea preocupaciones medioambientales a nivel mundial. Un informe reciente de MusicTank [30], se

señala que tan solo YouTube representa el 0,1% del consumo mundial de energía, y por tanto, recomienda un almacenamiento en nube cercano a los consumidores a fin de reducir las repercusiones medioambientales de los servicios de transmisión de música en tiempo real.

En la actualidad, se han tomado medidas para alentar a los operadores de centros de datos en nube a minimizar su consumo energético. En 2009, por ejemplo, la Comisión Europea publicó un Código de conducta sobre eficiencia energética en los centros de datos [31]. Se trata de una serie de medidas voluntarias destinadas a mejorar la eficiencia energética en el diseño y funcionamiento de los centros de datos.

Entre las medidas para reducir los costes, cabe señalar la construcción de centros de datos con sistemas de refrigeración, naturales y pasivos. Según las técnicas de almacenamiento distribuido, las cargas de procesamiento de datos pueden trasladarse a zonas geográficas donde el suministro eléctrico resulta menos costoso. Además, la arquitectura flexible de la nube permite reducir la duplicación.

- ***Normas de seguridad***

  La seguridad del entorno en el que se realiza la computación en nube preocupa no solo a los usuarios, sino también a los gobiernos que tratan de facilitar la implantación de la nube, de ahí la necesidad, que los proveedores de servicios en nube utilicen normas de seguridad existentes, como la ISO/CEI 27001 para sistemas de seguridad de la información o la SAS70, que prevén certificación y auditoría externa.

  Últimamente, se han puesto en marcha iniciativas de normalización destinadas específicamente a la nube. Para ejemplo se tiene a la Cloud Security Alliance que se encuentra desarrollando buenas prácticas en la industria y mejorando la transparencia para los usuarios de la nube. En el Sector de Normalización de las Telecomunicaciones, la Comisión de Estudio lleva trabajando sobre la seguridad en la nube, para desarrollar directrices y requisitos aplicables a diferentes ámbitos, como la gestión de identidad.

  El sector público es la tercera fuente de normas de seguridad sobre la nube. En algunos países, las autoridades públicas están comenzando a adoptar soluciones de computación en nube propuestas por el sector privado, pero solo cuando dichos

servicios están acreditados por terceros, certificando que ofrecen suficientes niveles de seguridad. Dado el volumen de contratación pública de productos y servicios de tecnologías de la información, las normas de seguridad impulsadas por los gobiernos acabarán probablemente influyendo en el desarrollo de los mercados. Si estas normas se vuelven demasiado específicas, podrían menoscabar la rentabilidad de la computación en nube al imponer requisitos innecesariamente estrictos.

- ***Facilitar los servicios en nube***

  ¿Qué medidas deberían tomar los gobiernos para facilitar la implantación y adopción de la computación en nube? Ya se han sugerido algunos planteamientos generales. Por ejemplo, en mayo de 2012, el Parlamento Europeo publicó un estudio en el que se identifican consejos para que los encargados de elaborar políticas faciliten la computación en nube, como acabar con los vacíos legales, mejorar las condiciones para todos los usuarios, dar respuesta a las preocupaciones sobre seguridad de las partes interesadas, fomentar la nube en el sector público y promover más investigación y desarrollo en el ámbito de la computación en nube.

1.3.2 POSIBLES SOLUCIONES

Considerando que el Ecuador tiene un vacío jurídico, al no contar con una normativa legal específica que regule y estandarice los servicios de Cloud Computing, que está siendo rápidamente acogido por las empresas y entidades gubernamentales del país, surge la necesidad imperante de que la Asamblea Nacional Legislativa haga una revisión urgente y proponga alternativas de modificación a las leyes existentes (Constitución de la República del Ecuador, Ley del Sistema Nacional de registro de Datos Públicos, Ley de comercio electrónico, firmas electrónicas y mensajes de datos) o la creación de una nueva ley basada en referentes y recomendaciones mundiales, con el propósito de crear un marco legal robusto y apropiado.

Mientras tanto, solo nos queda ampararnos en alternativas legales existentes, como lo son el contrato, los acuerdos de Nivel de Servicio (SLA) o en cualquier otro documento que se establezca entre el cliente y el proveedor, y en donde se estipule claramente aspectos como la protección de los datos, la seguridad en el

almacenamiento o en las transferencias, el acceso de las autoridades policiales, la preservación de la confidencialidad y no divulgación; como única herramienta jurídica para el amparo en cualquier tema legal futuro.

Para Gonzalo Salas senior manager de SIA International, para el caso particular de España y a falta de una normativa internacional vigente, el Contrato se constituye en la parte medular de la computación en la nube como la voluntad común de los contratantes elevados a norma vinculante que busca mitigar los potenciales riesgos expuestos por Gartner. Según el experto, en la computación en la nube, se encuentran embebidos servicios de hardware, software, comunicaciones y servicios profesionales, que deben ser debidamente regulados dentro del contrato mediante los siguientes elementos básicos, que a criterio personal se constituyen en posibles soluciones a los potenciales riesgos de la adopción de la computación en la nube por entidades del sector público ecuatoriano:

- ***Descripción detallada del servicio***.- Debe especificar el objeto y causas del contrato como preámbulo de los derechos y obligaciones que posteriormente se expondrán en las cláusulas del contrato. Por la naturaleza propia de la computación en la nube, es fundamental a efectos de estricta seguridad jurídica, indicar la ubicación del prestador del servicio, la localización de los servicios, el emplazamiento de las infraestructuras donde vayan a estar desplegadas las máquinas y plataformas y el tipo de servicios contratados.

- ***Tipo de servicio del cliente, soportados sobre el modelo cloud***.- Especificar particularidades sobre el contrato y/o servicio (elementos en materia de seguridad, accesibilidad, monitorización y auditabilidad entre otros) e inventariar todos los tipos de servicio que vayan a ser soportados, para posteriormente marcar las obligaciones de manera particular y no con carácter general y de esta manera, ganar en la gobernanza del servicio.

- ***Descripción del tipo de infraestructura.-*** Dependiendo del tipo de infraestructura, el contrato llevará un determinado tipo de cláusula, por lo que es importante a los efectos de catalogación del contrato, objeto y causa, describir el tipo de infraestructura contratada: IaaS, PaaS o SaaS

- ***Capacidad del servicio.-*** Dependiendo del tipo de infraestructuras, deberá reflejarse los umbrales máximos de capacidad del servicio contratado. El proveedor

deberá contar con herramientas de monitorización para medir capacidades y rendimientos a los efectos de certificar la correcta prestación de los servicios contratados.

- ***Gobernanza***.- A fin de garantizar una cooperación eficiente entre las partes y evitar llegar a situaciones de tener que aplicar las penalizaciones, cláusulas penales del contrato y/o la propia resolución del mismo, se recomienda crear Comités de Gobernanza a través de los cuales se supervise: la correcta prestación del servicio y cumplimiento de acuerdos de nivel de servicio, la gestión de cambio, la gestión de riesgos, la gestión y reporte de auditorías y validación y Aprobación de facturas, entre otros.

- ***Auditorías***.- Se debe contemplar la posibilidad de realizar auditorías ya sea por parte de entidades independientes solventes y sometidas a fuertes políticas de autonomía, ética e independencia. Estas podrán ser totales o parciales y dependiendo de la gravedad de los hechos significativos o vulnerabilidades detectadas, podrán ser causa de resolución del contrato.

- ***Ejecución y calidad de los servicios***.- A lo largo de toda la duración del Contrato, el proveedor debe comprometerse a garantizar servicios de calidad, conforme a los Acuerdos de Nivel de Servicio; medidas de seguridad, conforme a los requerimientos de seguridad de la información expuestos, siendo éstas obligaciones de resultado.

- ***Entrada en vigor y duración del servicio***.- Se debe especificar la vigencia y duración del contrato, de igual forma se debe recalcar el tiempo que el proveedor tardará en devolver los servicios o en su defecto garantizará la destrucción de la información almacenada en sus sistemas de información.

- ***Reversibilidad***.- El proveedor debe comprometerse a garantizar la reversibilidad parcial o total de la externalización de los servicios sin atadura alguna y en las mejores condiciones ya sea a cuenta propia del cliente o por parte de un tercer proveedor, para lo cual se recomienda incorporar a modo de acuerdo de intención la obligación del proveedor de proporcionar recursos, elementos o materiales portables para la transferencia exitosa a la otra ubicación informática sin costo u obligación adicional alguna (adquisición previa de programas de software).

- ***Confidencialidad del servicio***.- A fin de que el proveedor se obligue de manera recíproca a guardar el debido secreto respecto de toda la documentación, conversaciones, modelos de negocio e información tratada entre las partes previa y durante la ejecución del contrato. Se sugiere evitar poner acuerdos de confidencialidad indefinidos ya que el ordenamiento jurídico tiende a castigar con la nulidad a las obligaciones perpetuas.

- ***Disponibilidad del servicio.-*** Siendo un elemento diferenciador de este modelo el acceso sin restricciones, debe estipularse que el servicio estará disponible 24 horas al día, 365 días al año. No obstante como los entornos deberán verse sometidos a procesos de mantenimiento, actualización y mejora, deberá pactarse las franjas horarias sobre las que se va a realizar dichas actividades con el menor impacto posible de cara al cliente, mismo que deberán estar claramente definidos en los acuerdos de nivel de servicio.

- ***Acuerdos de nivel de servicio***.- Elemento típico de este tipo de contratos. Junto a los mismos se deben concretar los sistemas de penalización por incumplimiento que pueden ser cláusulas penales o daños y perjuicios. Es de vital importancia la definición de los procedimientos, estándares y mecanismos que permitan la correcta evaluación y cumplimiento de manera efectiva y objetiva de los acuerdos de nivel de servicio, ya sea mediante la incorporación de soluciones en el mercado como la Gestión de Nivel de Servicios (SLM) que permita la automatización del cálculo y seguimiento de los Acuerdos de Nivel de Servicio.

- ***Requerimientos legales***.- Según el tipo de servicio, se puede encontrar con distintas casuísticas y elementos a tener en consideración, desde la posibilidad de acceso a los distintos tipos de inspectores (Contraloría General del Estado, la Superintendencia de Bancos, etc.), pasando por el cumplimiento de requerimientos técnicos en materia de accesibilidad, comunicación, auditoría, como la configuración o pre-constitución de todo un conjunto de elementos que permitan acreditar el cumplimiento de algún tipo de requerimiento normativo.

- ***Propiedad intelectual***.- La protección de la propiedad intelectual del software debe ser un pilar clave a efectos de eliminar riesgos legales de uso de software sin licencia y la reversibilidad del servicio.

- ***Seguridad de la información***.- Misma que entre otras cosas debe contemplar a cuenta del proveedor de servicio: deber de secreto del personal; autorizaciones y control de acceso; protección de las instalaciones; medidas de seguridad por defecto; integridad y actualizaciones de los sistemas; procedimientos de gestión de cambios; protección de la información almacenada y en tránsito; medidas de prevención ante otros sistema de información interconectados; registro de incidencias; registros de actividad; plan de continuidad de negocio y procedimientos de recuperación frente a desastres

- ***Protección de datos de carácter personal***.- Considerando que la computación en la nube se define como aplicaciones entregadas como servicio a través de Internet, se recomienda que previamente a la suscripción de un contrato, se realice una evaluación de riesgos adecuada, incluyendo las ubicaciones de los servidores donde se tratan los datos y la consideración de los riesgos y ventajas desde la perspectiva de la protección de datos de carácter personal.

- ***Cesión-Subcontrato***.- El proveedor se debe comprometer, por una parte a no transferir o ceder, por ninguna causa y bajo ninguna forma, el Contrato o cualquiera de sus derechos y obligaciones a un tercero y, por otra, a no confiar a un tercero la ejecución total o parcial de sus obligaciones contractuales, sin la autorización previa y por escrito del cliente. En el caso de cesión parcial o total el proveedor se debe comprometer a notificar y garantizar que se respetará los términos y condiciones del Contrato, pudiendo el cliente rescindir el Contrato.

- ***Responsabilidades y obligaciones***.- El proveedor debe comprometerse a ejecutar los Servicios con toda la diligencia debida de su sector profesional, de ser el caso, asumir toda responsabilidad de las consecuencias que se deriven de sus faltas, errores u omisiones, así como de las faltas, errores u omisiones de sus Subcontratistas.

- ***Seguro***.- El proveedor debe estar asegurado con respecto de su responsabilidad civil general y su responsabilidad civil profesional con una empresa de reconocida solvencia. Además debe comprometerse a mantener esos seguros a lo largo de la duración del Contrato, pero también para cubrir los siniestros que tengan origen en los hechos acaecidos antes del cese del contrato pero conocidos después de la rescisión del mismo, en particular mediante el pago de las primas, y a aportar prueba de ello.

- ***Ley Aplicable y Fuero***.- Se recomienda que en caso de falta de previsión, sería de aplicación la normativa legal vigente ecuatoriana que de forma indirecta se relacione con la computación en la nube, más específicamente: la Constitución de la República del Ecuador, la Ley del Sistema Nacional de registro de Datos Públicos y la ley de comercio electrónico, firmas electrónicas y mensajes de datos.

A continuación se listan las posibles soluciones propuestas por los líderes del sector: la organización internacional CSA (Cloud Security Alliance) y el instituto norteamericano NIST (National Institute of Standards and Technology).

- La Cloud Security Alliance en su informe "Principales Amenazas en la Nube" [28] plantea las siguientes recomendaciones de acuerdo a su amenaza:

AMENAZA	RECOMENDACIÓN
Abuso y mal uso de la computación en la nube	• implementar un sistema de registro de acceso más restrictivo • coordinar y monitorizar el fraude en tarjetas de crédito • monitorizar el tráfico de clientes para la detección de posibles actividades ilícitas • comprobar las listas negras públicas para identificar si los rangos IP de la infraestructura han entrado en ellas
Interfaces y API poco seguros	• analizar los problemas de seguridad de las interfaces de los proveedores de servicio • asegurarse que la autenticación y los controles de acceso se implementan teniendo en cuenta el cifrado de los datos
Amenaza interna	• especificar cláusulas legales y de confidencialidad en los contratos laborales • determinar los posibles problemas en los procesos de notificación

Problemas derivados de las tecnologías compartidas	• diseñar buenas prácticas para la instalación y configuración • monitorizar los entornos para detectar cambios no deseados en las configuraciones o la actividad • proporcionar autenticación fuerte y control de acceso para el acceso de administración • adecuar los acuerdos de nivel de servicio para controlar el parcheado y la corrección de vulnerabilidades
Pérdida o fuga de información	• implementar API potentes para el control de acceso • proteger el tránsito de datos mediante el cifrado de los mismos • analizar la protección de datos tanto en tiempo de diseño como en tiempo de ejecución • proporcionar mecanismos potentes para la generación de claves, el almacenamiento y la destrucción de la información • definir, por contrato, la destrucción de los datos antes de que los medios de almacenamiento sean eliminados de la infraestructura, así como la política de copias de seguridad
Secuestro de sesión o servicio	• prohibir, mediante políticas, compartir credenciales entre usuarios y servicios • aplicar técnicas de autenticación de doble factor siempre que sea posible • monitorizar las sesiones en busca de actividades inusuales

Riesgos por desconocimiento	• tener acceso a los logs (registros de actividad) de aplicaciones y datos • estar al corriente, total o parcialmente, de los detalles de la infraestructura • monitorizar y recibir alertas sobre el uso de información crítica

Tabla 1.3.2.1: Recomendaciones según la CSA.

- Según la Guía sobre Seguridad y Privacidad en Nubes Públicas, publicada por el Instituto Nacional de Normas y Tecnología (NIST) propone las siguientes recomendaciones de seguridad por área:

ÁREA	RECOMENDACIÓN
Gobernanza	• Implantar políticas y estándares en la provisión de servicios cloud. • Establecer mecanismos de auditoría y herramientas para que se sigan las políticas de la organización durante el ciclo de vida.
Cumplimiento	• Entender los distintos tipos de leyes y regulaciones y su impacto potencial en los entornos cloud. • Revisar y valorar las medidas del proveedor con respecto a las necesidades de la organización.
Confianza	• Incorporar mecanismos en el contrato que permitan controlar los procesos y controles de privacidad empleados por el proveedor.
Arquitectura	• Comprender las tecnologías que sustentan la infraestructura del proveedor para comprender las implicaciones de privacidad y seguridad de los controles técnicos.
Identidad y control de acceso	• Asegurar las salvaguardas necesarias para hacer seguras la autenticación, la autorización y las funciones de control de acceso.

Aislamiento de software	• Entender la virtualización y otras técnicas de aislamiento que el proveedor emplee y valorar los riesgos implicados
Disponibilidad	• Asegurarse que durante una interrupción prolongada del servicio, las operaciones críticas se pueden reanudar inmediatamente y todo el resto de operaciones, en un tiempo prudente.
Respuesta a incidentes	• Entender y negociar los contratos de los proveedores así como los procedimientos para la respuesta a incidentes requeridos por la organización.

Tabla 1.3.2.2: Recomendaciones según la NIST

Como se puede evidenciar, el análisis de problemas y sus posibles soluciones pueden ser analizadas desde diferentes perspectivas y particularidades, en todo caso desde el punto de vista del consumidor y a falta de normativa legal se debería optar por la que más se adapte a los intereses de la organización previo el respectivo análisis de riesgo de la Infraestructura como Servicio de la Computación en la Nube.

RESUMEN

En este capítulo se analizó el estudio del arte de los servicios de Cloud Computing, tomando como base trabajos o iniciativas de principales organismos internacionales que impulsan la adopción o despliegue de la Computación en la Nube independientemente del tipo de entidad: pública, privada o gubernamental. En este análisis se hizo hincapié en la gestión de riesgos, determinándose que el nivel de riesgo variará considerablemente en función del tipo de arquitectura de nube que se esté considerando, que para el caso particular del presente trabajo es la Infraestructura como Servicios (IaaS).

En el diagrama causa – efecto (FishBone) de la Figura 1.3.2.1 se resumen y categorizan los potenciales riesgos que serán analizados durante el desarrollo del Modelo de Gestión de Riesgos de Infraestructura como Servicios (IaaS) de Cloud Computing aplicado a entidades del sector público ecuatoriano.

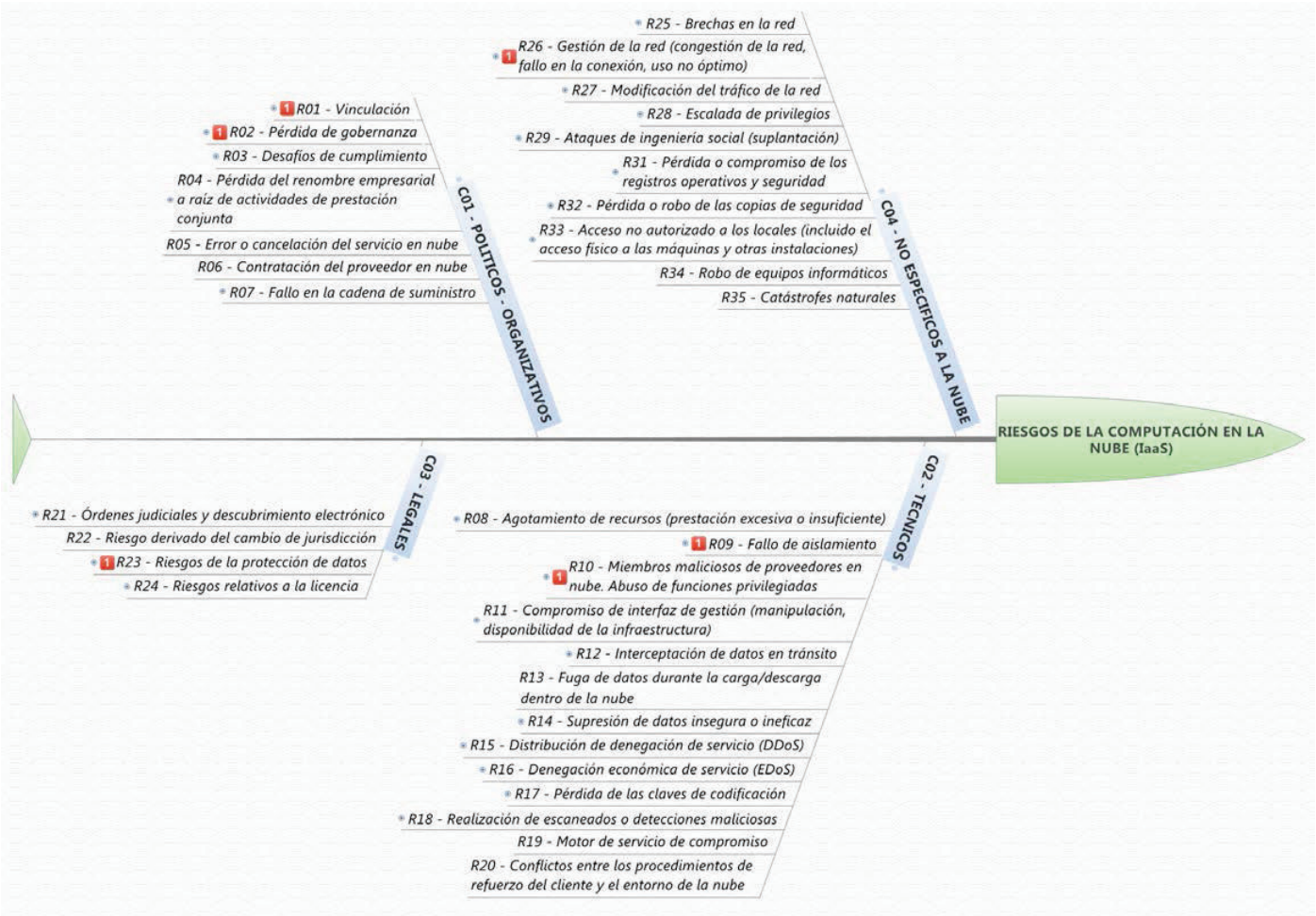

Figura 1.3.2.1 Potenciales Riesgos de Infraestructura como Servicios (IaaS) de Cloud Computing.

CAPITULO 2

DESARROLLO DEL MODELO DE RIESGOS DE SERVICIOS DE CLOUD COMPUTING BASADOS EN COBIT, OCTAVE E ISO27000.

En el capítulo anterior se analizó el estado del arte de la Gestión de Riesgos de Servicios de Cloud Computing, basados en numerosos estudios realizados por las grandes corporaciones y organizaciones que impulsan la migración o adopción de la computación en la nube como lo son la NIST, la CSA, ISACA, ENISA, ALAI, CET.LA, IBM, CISCO, etc.

Análisis que ha permitido identificar y valorar los potenciales riesgos relacionados con la computación en la nube, más específicamente con el modelo de Infraestructura como Servicio (IaaS), ahora solo queda hacerles frente mediante el desarrollo de un modelo de gestión de riesgos de servicios de Cloud Computing, ya que dado su calificativo de tecnología emergente, hasta la presente no se dispone de normativa que la regule.

En la actualidad existe un sin número de metodologías, estándares o normas que tratan el análisis y la gestión de riesgos (BS 7799 – 3, CRAMM, COBIT, ISO 27005, ISO 31010, ITIL, MAGERIT, OCTAVE, RISK IT, UNE 71504), tanto local como internacional. Normas al alcance de cualquier organización como guías o buenas prácticas bajo un proceso estandarizado y normalizado, que a la postre permitirá alcanzar los resultados esperados. Sin embargo, ninguno abarca los potenciales riesgos relacionados con la computación en la nube, misma que cada vez se extiende a nivel global como solución emergente a las acuciantes necesidades de almacenamiento y procesamiento ilimitados a bajo costo, tan requeridas por las organizaciones.

En el presente capítulo, se seleccionará y analizara las normas, estándares o mejores prácticas que mejor se alineen con la normativa local (ISO IEC27000) y que aporten elementos generales importantes para la gestión de riesgos del modelo

de servicio en la nube propuesto (OCTAVE), para finalmente establecer una estrategia de integración (COBIT), cuyo resultado será la determinación de controles que permitan mitigar los potenciales riesgos que implicaría la adopción o migración a la nube por parte de las entidades del sector público ecuatoriano.
La descripción de cada metodología o estándar se ha basado en documentos oficiales adquiridos o disponibles en su respectivo sitio web.

2.1 ANÁLISIS DE LOS MARCOS DE TRABAJO COBIT, OCTAVE E ISO27000 PARA LA GESTIÓN DE RIESGOS

En esta sección se revisará tres normas, métodos o conjuntos de buenas prácticas que proveerán lineamientos para ejecutar actividades enfocadas a la gestión de los riesgos de Infraestructura como Servicios (IaaS) de Cloud Computing identificadas, analizadas y evaluadas en el capítulo 1, ellas son: la norma NTE INEN-ISO/IEC 27005:2012, el método OCTAVE y la buenas prácticas de COBIT.

2.1.1 OCTAVE

Del inglés Operationally Critical Threat, Asset And Vulnerability Evaluation. Es una técnica efectiva de evaluación de riesgos desarrollada en el Centro de Coordinación CERT en Carnegie Mellon University, como un conjunto de herramientas, técnicas y métodos para la evaluación del riesgo, basada en seguridad de la información estratégica y la planificación, que toma en cuenta la definición de los activos incluyendo: personas, hardware, software, información y sistemas [32].
OCTAVE se enfoca en el riesgo organizacional – principalmente en los aspectos relacionados con el día a día – y su objetivo principal son los temas relativos a la estrategia y la práctica; igualmente proporciona una línea base que se puede utilizar para enfocar la mitigación y mejorar actividades; además, equilibra los riesgos operativos, las prácticas de seguridad y la tecnología, lo cual permite tomar decisiones para la protección de la información basado en los riesgos que atentan contra la confidencialidad, integridad y disponibilidad de información sensible o crítica para la organización [32].
Para OCTAVE el factor humano cumple un rol importante en el cumplimiento de la misión organizacional e implementación de esta metodología, por lo que considera

que los empleados de todos los niveles deben entender qué activos relacionados con la información son importantes y cómo deben protegerlos. Que a la postre permite a OCTAVE la conformación de un equipo mixto, compuesto de personas de las áreas de negocios y de TI durante su implementación. Esta configuración explica el hecho de que los funcionarios del negocio son los más indicados para identificar qué información es importante en los procesos y cómo se usa dicha información; por su parte, el equipo de TI, es el que conoce la configuración de la infraestructura y las debilidades que pueden tener, estos dos puntos de vista son importantes para tener una visión global de los riesgos de seguridad de los servicios de TI.

OCTAVE, al ser un conjunto de criterios a partir de los cuales se pueden desarrollar diversas metodologías, se acopla perfectamente en el desarrollo del Modelo de Gestión de Riesgos de Infraestructura como Servicios (IaaS) de Cloud Computing aplicado a entidades del sector público ecuatoriano [33], mediante la integración de normas o mejores prácticas disponibles en el mercado.

Los criterios de OCTAVE que definen el enfoque para evaluaciones de riesgos de seguridad de la información son los principios (Principle), los atributos (Attribute) y las salidas (Output) [33].

Los principios son los conceptos fundamentales que impulsan la naturaleza de la evaluación y que definen la filosofía detrás del proceso de evaluación. Configuran el enfoque de la evaluación y sirven de base para el proceso de evaluación. Por ejemplo, “La metodología debe ser auto-dirigida” es uno de los principios de OCTAVE. El concepto de auto-dirigida significa que las mismas personas de la organización están en la mejor posición de dirigir la evaluación y tomar decisiones. Los requisitos de la evaluación están incorporados en los atributos y salidas.

Los atributos son las cualidades distintivas o características de la evaluación. Ellos son los requisitos que definen los elementos básicos del enfoque OCTAVE y definen lo que es necesario hacer para una evaluación exitosa tanto desde la perspectiva del proceso como de la organización.

Como se puede ver en la Tabla 2.1.1.1, los atributos se derivan de los principios de OCTAVE. Por ejemplo, uno de los atributos de OCTAVE es que un equipo interdisciplinario (el equipo de análisis) constituido por personal de la organización

este dirigiendo la evaluación. El principio detrás de la creación de un equipo de análisis es “La metodología debe ser auto-dirigida”.

PRINCIPIOS (PRINCIPLE)	ATRIBUTOS (ATTRIBUTE)
La metodología debe ser auto-dirigida	RA.1 Equipo de análisis RA.2 Capacidades del equipo de análisis
Las medidas deben ser adaptables a las necesidades	RA.3 Catálogo de prácticas RA.4 Perfil genérico de amenazas RA.5 Catálogo de vulnerabilidades
El proceso debe ser definido	RA.6 Actividades de evaluación definidas RA.7 Documentación de los resultados de la evaluación RA.8 Alcance de la evaluación
El proceso debe ser continuo	RA.9 Próximos pasos RA.3 Catálogo de prácticas
El proceso debe seguirse con visión de futuro	RA.10 Enfoque en riesgos
El proceso debe centrarse en un reducido número de riesgos críticos	RA.8 Alcance de la evaluación RA.11 Actividades enfocadas
Gestión integrada	RA.12 Aspectos organizativos y tecnológicos RA.13 Participación de negocio y de áreas tecnológicas RA.14 Participación de la alta dirección
Comunicación abierta	RA.15 Enfoque colaborativo
Perspectiva global	RA.12 Aspectos organizativos y tecnológicos RA.13 Participación de negocio y de áreas tecnológicas
Equipo de trabajo	RA.1 Equipo de análisis RA.2 Capacidades del equipo de análisis RA.13 Participación de negocio y de áreas tecnológicas RA.15 Enfoque colaborativo

Tabla 2.1.1.1: Criterios de OCTAVE - Principios y Atributos

Por último, las salidas son los resultados requeridos de cada fase de evaluación. Definen los resultados que un equipo de análisis debe alcanzar durante cada fase. Hay más de un conjunto de actividades que pueden producir las salidas de OCTAVE; por esta razón, no se especifica un conjunto único de actividades. Las salidas definen los resultados que un equipo de análisis debe alcanzar durante la evaluación y están organizados de acuerdo a las tres fases, como se evidencia en la Tabla 2.1.1.2.

FASES (PHASE)	SALIDAS (OUTPUT)
Visión organizativa	RO1.1 Activos críticos RO1.2 Requerimientos de seguridad para los activos críticos RO1.3 Amenazas sobre los activos críticos RO1.4 Prácticas de seguridad actuales RO1.5 Vulnerabilidades organizativas actuales
Visión tecnológica	RO2.1 Componentes clave RO2.2 Vulnerabilidades tecnológicas actuales

Estrategia y desarrollo del plan	RO3.1 Riesgos sobre activos críticos RO3.2 Medidas contra los riesgos RO3.3 Estrategia de protección RO3.4 Planes de mitigación del riesgo

Tabla 2.1.1.2: Criterios de OCTAVE – Salidas

De acuerdo a la Figura 2.1.1.1, el proceso de evaluación contemplado por OCTAVE se divide en tres fases (F) y ocho procesos (P), que se describen a continuación:

- ***Fase 1: Visión organizativa - Construcción de los Perfiles de amenazas Basados en Activos***.- Esta es una evaluación de la organización. El equipo de análisis determina lo que es importante para la organización (los activos relacionados con la información) y lo que se está haciendo actualmente para proteger esos activos. Posteriormente, el equipo selecciona aquellos activos que son más importantes para la organización (activos críticos) y describe los requisitos de seguridad para cada activo crítico. Por último, se identifican las amenazas a cada activo crítico, creando un perfil amenaza para ese activo.

    - ***Proceso 1 – Identificar conocimiento de la alta dirección***.- Se identifican los activos importantes, amenazas percibidas, los requisitos de seguridad, las prácticas actuales de seguridad y vulnerabilidades de la organización desde la perspectiva de los altos directivos.

    - ***Proceso 2 – Identificar conocimiento de la dirección de áreas operativas***.- Se identifican los activos importantes, amenazas percibidas, los requisitos de seguridad, las prácticas actuales de seguridad y vulnerabilidades de la organización desde la perspectiva de los administradores de las áreas operacionales.

    - ***Proceso 3 – Identificar conocimiento del personal de áreas operativas y de TI***.- Se identifican los activos importantes, amenazas percibidas, los requisitos de seguridad, las prácticas actuales de seguridad y vulnerabilidades de la organización desde la perspectiva del personal de áreas operativas y de TI

    - ***Proceso 4 – Crear perfiles de amenazas***.- El equipo de análisis evalúa la información de los procesos de 1 a 3, selecciona los activos críticos, refina los requisitos de seguridad asociados y se identifican las amenazas a esos activos para la creación de perfiles de amenaza.

- ***Fase 2: Visión tecnológica - Identificación de la infraestructura de vulnerabilidades***.- Esta es una evaluación de la infraestructura de información. El equipo de análisis examina e identifica vulnerabilidades y sus componentes tecnológicos relacionada con cada activo crítico, para posteriormente determinar la medida en que cada clase de componente es resistente a los ataques. Las vulnerabilidades de tecnología son las debilidades en los sistemas, dispositivos y componentes que pueden conducir directamente a la acción no autorizada

    - ***Proceso 5 – Identificar componentes clave***.- El equipo de análisis identifica los sistemas de información y componentes tecnológicos claves para cada activo crítico. Los casos específicos se seleccionan para su evaluación.

    - ***Proceso 6 – Evaluar componentes seleccionados***.- El equipo de análisis examina los principales sistemas y componentes tecnológicos vulnerables, para lo cual se utilizan herramientas de vulnerabilidad (software, listas de verificación, scripts). Los resultados se analizan y se resumen, de acuerdo a la importancia de los activos críticos y sus perfiles de amenaza.

- ***Fase 3: Estrategia y desarrollo del plan***.- Durante esta parte de la evaluación, el equipo de análisis identifica los riesgos de los activos críticos de la organización y decide qué hacer con ellos. El equipo crea una estrategia de protección para la organización y planes de mitigación para hacer frente a los riesgos de los activos críticos, en base a un análisis de la información recopilada.

    - ***Proceso 7 – Analizar los riesgos***.- El equipo de análisis identifica el impacto de las amenazas a los activos críticos, crea criterios para evaluar esos riesgos, y evalúa los impactos en base a esos criterios. Esto produce un perfil de riesgo para cada activo crítico.

    - ***Proceso 8 – Diseñar la estrategia de protección.-*** El equipo de análisis crea una estrategia de protección y un plan de mitigación para la organización y los activos críticos, en base al análisis de la información recopilada. Los altos directivos luego revisan, modifican y aprueban la estrategia y los planes.

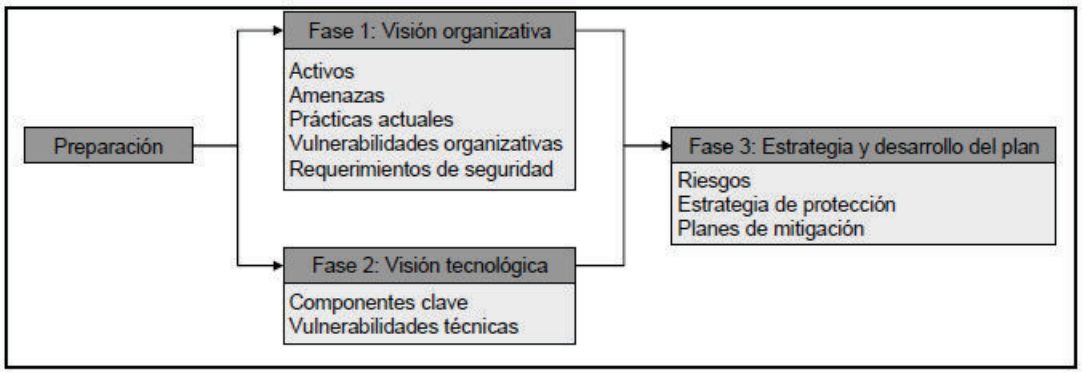

Figura 2.1.1.1 Fases metodología Octave.

Faces y proceso que se adaptan a necesidades particulares de la organización y a cada método establecido por OCTAVE, ver Tabla 2.1.1.3. Las tres metodologías de OCTAVE publicadas a la fecha de este documento por el Software Engineering Institute (SEI) de la Universidad de Carnegie Mellon, se listan a continuación:

- ***OCTAVE***.- Metodología original, definida para grandes organizaciones.
- ***OCTAVE-S***.- Metodología definida para pequeñas organizaciones.
- ***OCTAVE Allegro***.- Metodología definida para analizar riesgos con un mayor enfoque en los activos de información, en oposición al enfoque en los recursos de información.

OCTAVE	OCTAVE-S	OCTAVE ALLEGRO
Fase 1 – Proceso 1 (F1P1)	Fase 1 – Proceso 1 (F1P1)	Fase 1 Establecer dirección: Establecer criterios de valoración de riesgos
Fase 1 – Proceso 2 (F1P2)		Fase 2 Perfilar activos: Desarrollar perfiles de activos de información
Fase 1 – Proceso 3 (F1P3)		Fase 2 Perfilar activos: Identificar recursos de información
Fase 1 – Proceso 4 (F1P4)	Fase 1 – Proceso 4 F1P4	Fase 3 Identificar amenazas: Identificar áreas de interés para el análisis
Fase 2 – Proceso 5 (F2P5)	Fase 2 – Proceso 5 F2P5	Fase 3 Identificar amenazas: Identificar escenarios de amenazas
Fase 2 – Proceso6 (F2P6)		Fase 4 Identificar y mitigar riesgos: Identificar riesgos
Fase 3 – Proceso 7 (F3P7)	Fase 3 – Proceso 7 F3P7	Fase 4 Identificar y mitigar riesgos: Analizar riesgos
Fase 3 – Proceso 8 (F3P8)	Fase 3 – Proceso 8 F3P8	Fase 4 Identificar y mitigar riesgos: Seleccionar enfoque de mitigación

Tabla 2.1.1.3: Fases y procesos métodos OCTAVE

La metodología de OCTAVE seleccionada como parte del marco de trabajo para el desarrollo del Modelo de Gestión de Riesgos de Infraestructura como Servicios (IaaS) de Cloud Computing aplicado a entidades del sector público ecuatoriano es OCTAVE-S, no por el tamaño de la organización en la que se aplicará, sino:

- Considerando la exploración limitada de la infraestructura tecnológica que provee este nuevo modelo de gestión de TI llamado Cloud Computing, donde la mayoría de servicios de software, plataformas o infraestructura de TI se encuentra externalizadas en un Proveedor de Servicios de na Nube (CSP), quienes no brinda las facilidades necesarias para ejecutar o interpretar los resultados de las herramientas de vulnerabilidad.

- El supuesto que el equipo de análisis conoce y entiende los elementos importantes, los requisitos de seguridad, las amenazas, vulnerabilidades y riesgos de adoptar la computación en la nube, ya sea a través experiencias o casos de estudios publicados por líderes del mercado que impulsan la adopción del Cloud Computing.

- A esto se suma, el fácil acoplamiento a otras normas y estándares para crear nuevas metodologías de gestión de riesgos; equipo de análisis interdisciplinario de 3 a 5 personas de la propia organización; se basa en los criterios del estándar con un enfoque en la práctica y evaluación de la seguridad basada en la información del riesgo; apoyado en un catálogo de buenas prácticas, encuestas, hojas de cálculos para obtener y captar información; se centra en una técnica de análisis basada en la planificación de escenarios; incorpora el criterio de probabilidad en el análisis de riesgos; y lo más importante proporciona guías de implementación.

2.1.2 ISO/IEC 27005

Norma relacionada con la *Tecnologías De La Información – Técnicas De Seguridad – Gestión Del Riesgo De Seguridad De La Información*, que proporciona directrices para la gestión de riesgos de seguridad de la información. Es compatible con los conceptos generales y controles especificados en la norma NTE INEN-ISO/IEC 27001 y NTE INEN-ISO/IEC 27002, y está diseñada para ayudar a la aplicación satisfactoria de elementos que permitan garantizar la seguridad de la información basada en un enfoque de gestión de riesgos ya que las primeras definen la necesidad de elaborar un análisis de riesgos pero no especifican directrices para

ello. Es aplicable a todo tipo de organizaciones que tengan la intención de gestionar los riesgos que podrían comprometer la seguridad de su información [34].

Está basada en los informes técnicos ISO/IEC TR 13335-3:1998 e ISO/IEC TR 13335-4:2000, que quedaron obsoletos desde su publicación. También está basada en la norma BS 7799-3:2006. El proceso de gestión de riesgos se describe en las siguientes 6 cláusulas [34]:

- ***Cláusula 7.-*** Establecimiento del contexto, en la que se definen los objetivos, el alcance y la organización para todo el proceso.

- ***Cláusula 8.-*** Valoración de riesgos, en la que se obtiene toda la información necesaria para conocer, valorar y priorizar los riesgos. Se divide en tres apartados:

    - Identificación de riesgos, que consiste en determinar qué puede provocar pérdidas a la Organización.

    - Estimación de riesgos, que consiste en utilizar métodos cuantitativos o cualitativos para obtener una cuantificación de los riesgos identificados, teniendo en cuenta los activos, las amenazas y las salvaguardas.

    - Evaluación de riesgos, que consiste en comparar los riesgos estimados con los criterios de evaluación y de aceptación de riesgos definidos en el establecimiento del contexto.

- ***Cláusula 9.-*** Tratamiento de riesgos, en la que se define la estrategia para tratar cada uno de los riesgos valorados: reducción, aceptación, evitación o transferencia.

- ***Cláusula 10.-*** Aceptación de riesgos, en la que se determinan los riesgos que se decide aceptar, y la justificación correspondiente a cada riesgo aceptado.

- ***Cláusula 11.-*** Comunicación de riesgos, en la que todos los grupos de interés intercambian información sobre los riesgos.

- ***Cláusula 12.-*** Monitorización y revisión de riesgos, en la que el análisis de riesgos se actualiza con todos los cambios internos o externos que afectan a la valoración de los riesgos.

El proceso de gestión de riesgos definido por la norma NTE INEN-ISO/IEC 27005:2012, se puede esquematizar en la Figura 2.1.2.1

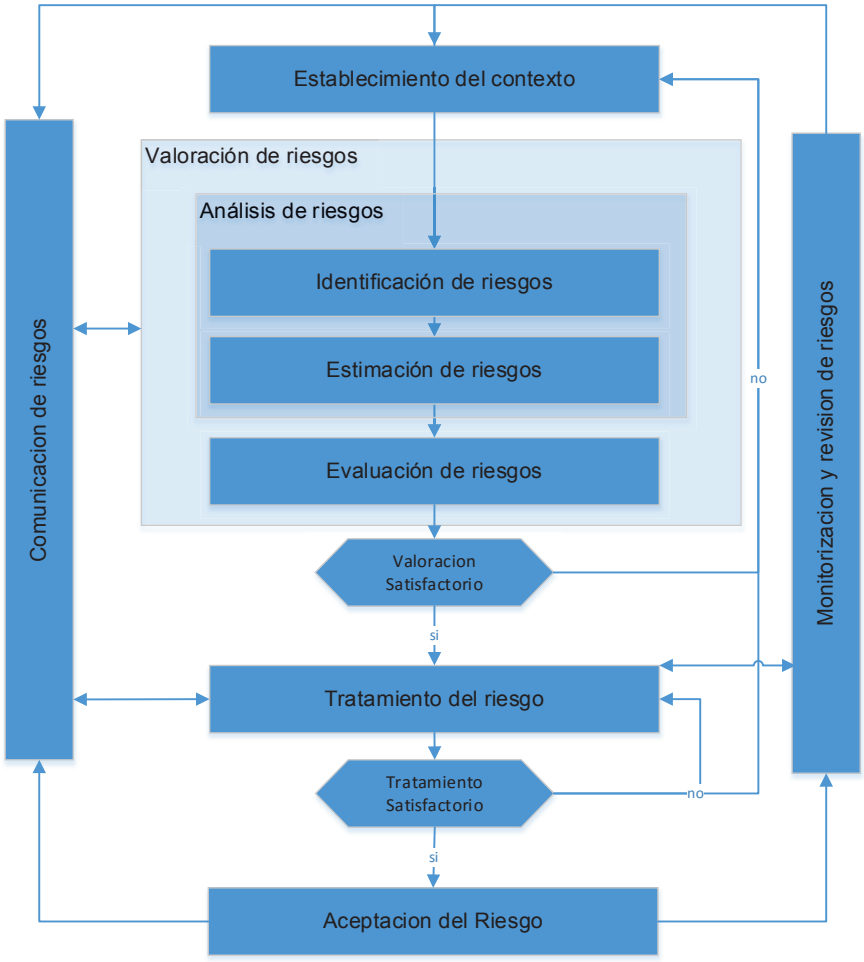

Figura 2.1.2.1 Modelo de gestión de riesgos según la NTE INEN-ISO/IEC 27005:2012 [34].

Donde se evidencia como el proceso de gestión de riesgos inicia con el establecimiento del contexto, seguido de la valoración del riesgo, que incluye la identificación, estimación y evaluación del riesgo. Posteriormente hay un punto de decisión donde se determina si hay suficiente información para determinar las acciones requeridas para modificar los riesgos a un nivel aceptable para luego completar el tratamiento del riesgo; si no hay información suficiente se debe realizar otra iteración, regresando al establecimiento del contexto. Cuando el tratamiento del riesgo no ha sido efectivo, es posible que no se obtenga un nivel de riesgo residual aceptable, entonces será necesaria otra iteración hacia el establecimiento del contexto. La aceptación del riesgo debe ser explícita por parte de la alta directiva de la organización. Durante todo el proceso de la gestión de riesgos, es necesario

que los riesgos y su tratamiento sean comunicados a la alta directiva y al personal operacional adecuado [35].

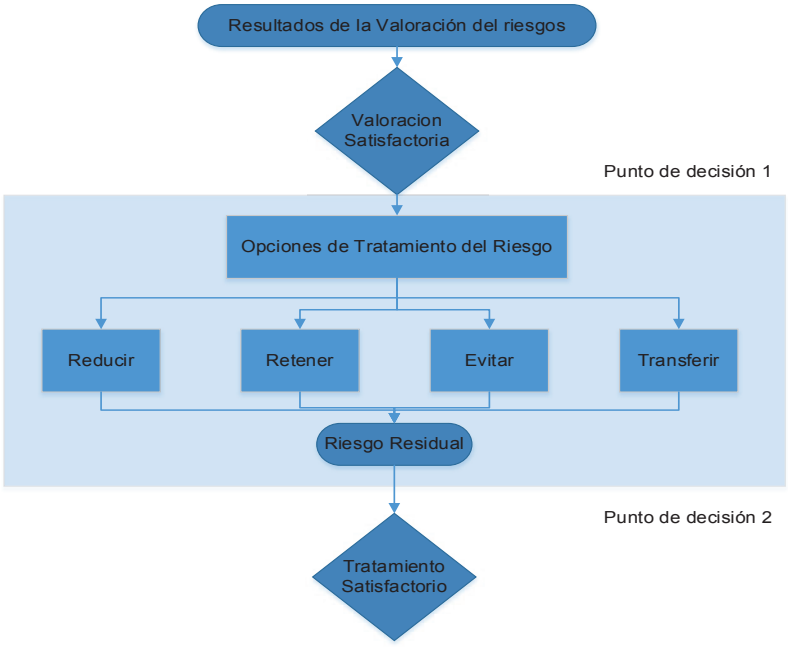

Figura 2.1.2.2 Actividades de tratamiento o gestión de riesgos [34]

Considerando que el presente trabajo se enfoca en la gestión de los riesgos de Cloud Computing identificados en el numeral 1.2.2, la parte medular de esta norma se centrará en la cláusula 9, es decir, definir estrategias para tratar dichos riesgos valorados, conforme al esquema de la Figura 2.1.2.2. Donde se deberá elegir grandes reducciones del riesgo con poco gasto, las elecciones costosas deberán ser justificadas. Una vez definido el tratamiento del riesgo, se debe definir el riesgo residual, esto puede requerir una iteración sobre la valoración del riesgo dependiendo de los efectos esperados del tratamiento. En caso de que el riesgo residual no sea aceptado, se requerirá una nueva iteración del tratamiento del riesgo.

Alineado con el estándar NTE INEN-ISO/IEC 27001:2012, el proceso de gestión de riesgos se considera iterativo, siguiendo el ciclo de Deming de la Figura 2.1.2.3, tema no contemplado en la elaboración del presente trabajo.

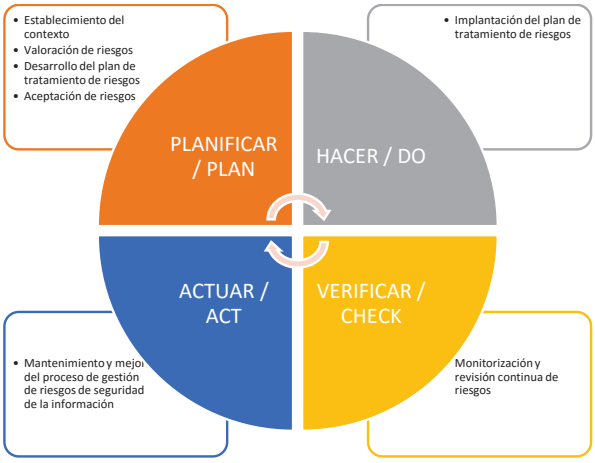

Figura 2.1.2.3 Ciclo de Deming aplicado a la Gestión de Riesgos.

2.1.3 COBIT

Del inglés *Control Objectives For Information And Related Technology.* La información como recurso clave empresarial desde que se crea hasta que se destruye, requiere que las organizaciones y la alta directiva se esfuercen, entre una de las cosas, en mantener los riesgos relacionados con las Tecnologías de la Información (TI) en un nivel aceptable. Para lo cual COBIT, provee de un marco de trabajo integral que ayuda a las empresas y organizaciones a crear el valor óptimo desde TI manteniendo el equilibrio entre la generación de beneficios y la optimización de los niveles de riesgos y el uso de recursos. COBIT al ser genérico y útil, puede ser adaptado a organizaciones de todos los tamaños, tanto comerciales, como sin ánimo de lucro o del Sector Público y en cualquier ubicación geográfica [36]. En la Figura 2.1.3.1 se muestra la familia de productos de COBIT5, que para el caso específico del presente trabajo nos enfocaremos en la relación que existe entre el marco de trabajo y la guía para riesgos.

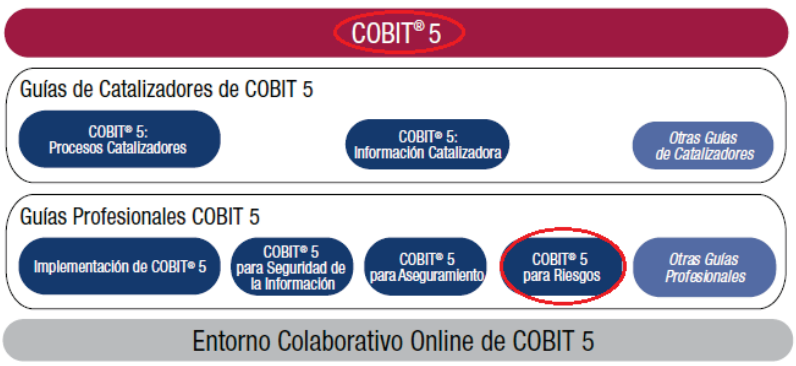

Figura 2.1.3.1 Familia de productos COBIT5 [36].

COBIT al ser un marco de referencia internacional es aceptado por la mayoría de organizaciones como buenas prácticas para el control de la información mediante la implementación de Gobierno de TI. COBIT ha sido diseñado para facilitar el uso de las TI desde un enfoque de inversión que debe estar bien administrado y está basado en los estándares y las mejores prácticas de la industria, y ayuda a salvar la brecha entre los riesgos del negocio, las necesidades de control y los aspectos propiamente técnicos. [37].

Figura 2.1.3.2 Principios de COBIT5 [36].

De acuerdo a la Figura 2.1.3.2, COBIT 5 se basa en cinco principios claves, que en conjunto, habilitan a la organización a construir un marco de gestión de gobierno y gestión efectivo que optimiza la inversión y el uso de información y tecnología para el beneficio de las partes interesadas. Principios que se describen a continuación:

- ***Satisfacer las Necesidades de las Partes Interesadas***.- Las empresas existen para crear valor para sus partes interesadas manteniendo el equilibrio entre la realización de beneficios y la optimización de los riesgos y el uso de recursos. Dado que toda organización tiene objetivos diferentes, pueden personalizar COBIT 5 para adaptarlo a su propio contexto, traduciendo metas corporativas de alto nivel en otras metas más manejables, específicas, relacionadas con TI y mapeándolas con procesos y prácticas específicos.

- ***Cubrir la Empresa Extremo-a-Extremo.-*** Es decir, integra el gobierno y la gestión de TI en el gobierno corporativo, cubriendo todas las funciones y procesos dentro de la organización y considerando que los catalizadores relacionados con TI para el gobierno y la gestión deben ser a nivel de toda la organización y de principio a fin.

- ***Aplicar un Marco de Referencia único integrado***.- Hay muchos estándares y buenas prácticas relativos a TI, ofreciendo cada uno ayuda para un subgrupo de actividades de TI. COBIT 5 se alínea a alto nivel con otros estándares y marcos de trabajo relevantes, y de este modo puede hacer la función de marco de trabajo principal para el gobierno y la gestión de las TI de la organización.

- ***Hacer Posible un Enfoque Holístico***.- Es decir, tiene en cuenta varios componentes interactivos (catalizadores) para un efectivo y eficiente gobierno y gestión de las TI de la organización, definidos en siete categorías de catalizadores: Principios, Políticas y Marcos de Trabajo; Procesos; Estructuras Organizativas; Cultura, Ética y Comportamiento; Información; Servicios, Infraestructuras y Aplicaciones; Personas, Habilidades y Competencias.

- ***Separar el Gobierno de la Gestión***.- Es decir, establece una clara distinción entre gobierno y gestión, ya que engloban diferentes tipos de actividades, requieren diferentes estructuras organizativas y sirven a diferentes propósitos.

    - ***Gobierno***.- Asegura que se evalúan las necesidades, condiciones y opciones de las partes interesadas para determinar que se alcanzan las metas corporativas equilibradas y acordadas; estableciendo la dirección a través de la priorización y la toma de decisiones; y midiendo el rendimiento y el cumplimiento respecto a la dirección y metas acordadas.

    - ***Gestión***.- La gestión planifica, construye, ejecuta y controla actividades alineadas con la dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales.

Adicionalmente, como se puede ver en la Figura 2.1.3.3, COBIT5 incluye un modelo de referencia de procesos que define y describe en detalle varios procesos de gobierno y de gestión, que normalmente encontramos en una organización relacionados con las actividades de TI. Dicho modelo no constituye el único modelo

de procesos posible, cada organización debe definir su propio conjunto de procesos, teniendo en cuenta su situación particular.

Figura 2.1.3.3 Modelo de referencia de procesos COBIT [36].

De acuerdo a la figura 2.1.3.3, el modelo de referencia de procesos de COBIT5 divide los procesos de gobierno y de gestión de la TI empresarial en dos dominios principales de procesos:

- ***Gobierno***.- Contiene cinco procesos de gobierno; dentro de cada proceso se definen prácticas de evaluación, orientación y supervisión (EDM).

- ***Gestión***.- Contiene cuatro dominios (APO, BAI, DSS, MEA), en consonancia con las áreas de responsabilidad de planificar, construir, ejecutar y supervisar (Plan, Build, Run and Monitor - PBRM), y proporciona cobertura de extremo a extremo de las TI.

Cada dominio contiene un número de procesos, estos a su vez requieren de actividades de “planificación”, “implementación”, “ejecución” y “supervisión”, que para el caso específico del presente trabajo serían los procesos y actividades del

dominio de gobierno EDM03 y de gestión APO12, mismos que permitirán gestionar los potenciales Riesgos de Infraestructura como Servicios (IaaS) de Cloud Computing en las entidades del sector público ecuatoriano.

De igual forma se tratará de abordar COBIT5 para Riesgos, el cual ha sido integrado en la Guías Profesionales de COBIT5 – como se puede evidenciar en la Figura 2.1.3.1 – para proporcionar una comprensión de cómo una gestión de riesgos TI eficiente optimiza el valor, junto con la eficacia y eficiencia de los procesos de negocio mejorando la conciencia entre todas las partes interesadas (internas y externas) gracias al uso de un marco común mundialmente aceptado y sostenible y el lenguaje para evaluación y respuesta al riesgo.

Desde la perspectiva de gestión de riesgos los procesos de soporte que COBIT5 aportaría en el desarrollo del presente Modelo de Gestión de Riesgos de Infraestructura como Servicios (IaaS) de Cloud Computing aplicado a entidades del sector público ecuatoriano, son:

- ***Gobierno – DM03 Asegurar la optimización del Riesgo***.- Abarca el entendimiento, la articulación y la comunicación del apetito y tolerancia al riesgo de la organización, y asegura la identificación y gestión del riesgo asociado al valor de la organización que está relacionado con el uso de TI y su impacto. Sus faces o prácticas de gobierno son:
    - ***EDM03.01 Evaluar la gestión de riesgos***.- Examinar y evaluar continuamente el efecto del riesgo sobre el uso actual y futuro de las TI en la organización. Considerar si el apetito de riesgo de la organización es apropiado y el riesgo sobre el valor de la organización relacionado con el uso de TI es identificado y gestionado.
    - ***EDM03.02 Orientar la gestión de riesgos***.- Orientar el establecimiento de prácticas de gestión de riesgos para proporcionar una seguridad razonable de que son apropiadas para asegurar que el riesgo en TI actual no excede el apetito de riesgo del Consejo.
    - ***EDM03.03 Supervisar la gestión de riesgos***.- Supervisar las metas y métricas clave de los procesos de gestión de riesgo y establecer cómo las desviaciones o los problemas serán identificados, seguidos e informados para su resolución.

- ***Gestión – APO12 Gestionar los riesgos***.- Abarca la identificación, evaluación y reducción continuo del riesgo relacionado con TI dentro de los niveles de tolerancia establecidos por la gerencia ejecutiva de la organización. La gestión de riesgos de la organización relacionada con TI debería ser integrada a la gestión de riesgos empresarial (ERM) global. Sus faces o prácticas de gobierno están representadas en la Figura 2.1.3.4 y son:

    - ***APO12.01 Recopilar datos***.- Identificar y recopilar datos relevantes para catalizar una identificación, análisis y notificación efectiva de riesgos relacionados con TI.

    - ***APO12.02 Analizar el riesgo***.- Desarrollar información útil para soportar las decisiones relacionadas con el riesgo que tomen en cuenta la relevancia para el negocio de los factores de riesgo.

    - ***APO12.03 Mantener un perfil de riesgo***.- Mantener un inventario del riesgo conocido y atributos de riesgo (incluyendo frecuencia esperada, impacto potencial y respuestas) y de otros recursos, capacidades y actividades de control actuales relacionados.

    - ***APO12.04 Expresar el riesgo***.- Proporcionar información sobre el estado actual de exposiciones y oportunidades relacionadas con TI de una forma oportuna a todas las partes interesadas necesarias para una respuesta apropiada.

    - ***APO12.05 Definir un portafolio de acciones para la gestión de riesgos***.- Gestionar las oportunidades para reducir el riesgo a un nivel aceptable como un portafolio.

    - ***APO12.06 Responder al riesgo***.- Responder de una forma oportuna con medidas efectivas que limiten la magnitud de pérdida por eventos relacionados con TI.

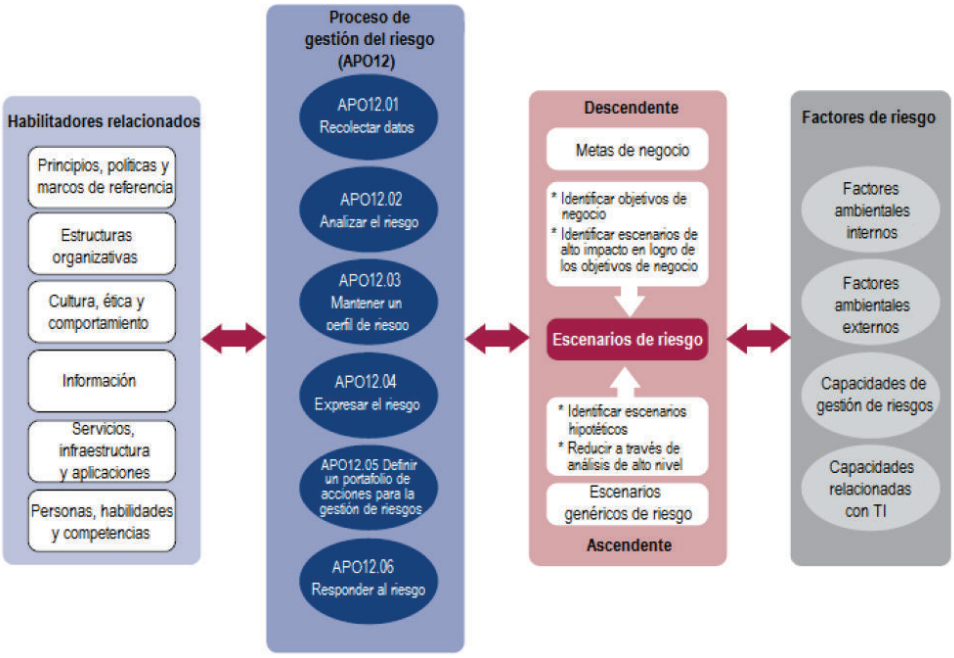

Figura 2.1.3.4 Panorama de la Gestión de Riesgos desde la perspectiva de COBIT5 [36].

COBIT5 a diferencia de la norma (ISO27005) y metodología (OCTAVE) analizadas anteriormente, se caracteriza por ser un marco de referencia paraguas para el gobierno y la gestión del riesgos.

COBIT5 asume una perspectiva más amplia de la gestión de riesgos de TI en comparación con la norma ISO/IEC 27005, esta última enfocada en la gestión de riesgos relacionados a la seguridad de información; perspectiva que en determinado momento puede ser una ventaja o una desventaja; que para el caso específico del presente trabajo constituye una desventaja ya que no se cuenta con el recurso humano y económico suficiente, razón por la cual se incorpora los proceso de ISO/IEC 27005 mapeados con los procesos y prácticas de COBIT para asegurar su alineamiento con los objetivos del negocio, su aceptación en toda la organización y un alcance completo [38].

Con respecto a la metodología OCTAVE, COBIT5 permite identificar oportunamente los riegos internos a los que la organización se encuentra expuesto ya que no minimizan el problema, más aún cuando gran parte de los riesgos provienen de “costumbres” internas de las organizaciones, además, que los principios, atributos y salidas están presentes en COBIT 5, ya sea a través de los

principios, el diseño conceptual del marco de referencia, el modelo de proceso o de las guías adicionales proporcionadas en el marco de referencia.

2.1.4 COMPARATIVAS Y JUSTIFICACIÓN

Analizados los marcos de trabajo para la gestión de riesgo, es necesario realizar una comparativa de las mismas con el objetivo de tener una visión general de los aportes que hacen cada uno de ellos, y que justifiquen su elección en el desarrollo del Modelo de Gestión de Riesgos de Infraestructura como Servicios (IaaS) de Cloud Computing aplicado a entidades del sector público ecuatoriano.

COBIT5, debido a su alto nivel, amplia cobertura y por estar basado en buenas prácticas de TI y Gobierno, se lo considera y utilizará como un marco de trabajo "integrador", que permitirá ubicar la norma ISO27005 y la metodología de OCTAVE bajo un mismo contexto, ayudando a enlazarlas y acoplarlas a los requerimientos del negocio, como se puede evidenciar en la Figura 2.1.4.1. Cabe indicar que COBIT5 se focaliza en lo que una organización necesita hacer, no cómo lo tiene que hacer. La audiencia objetivo es la alta gerencia, los gerentes funcionales, los gerentes de TI y los auditores [38].

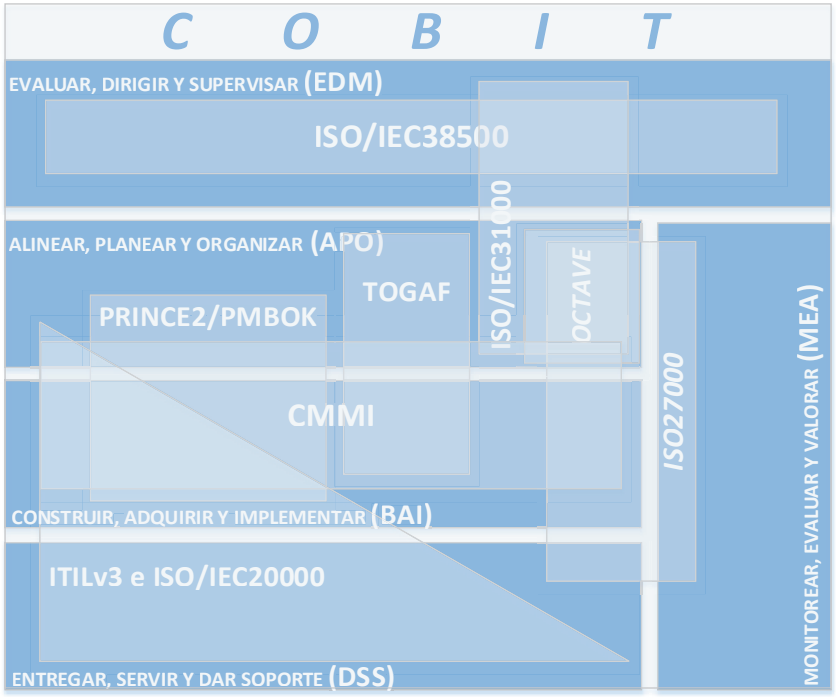

Figura 2.1.4.1 COBIT5 marco integrado ISO27005 y OCTAVE.

Mientras que la norma NTE INEN-ISO/IEC 27005:2012 al ser un estándar internacionalmente reconocido, solamente provee las pautas generales de ***¿qué hacer?*** para llevar a cabo un adecuado análisis, evaluación y gestión de riesgos; el ***¿Cómo hacerlo?***, es responsabilidad de la metodología OCTAVE la cual provee los pasos exactos para dicho fin. Por lo tanto, es posible seguir un estándar como guía o marco de trabajo dentro de un análisis y gestión de riesgos y utilizar una metodología en particular para llevarla a cabo [34].

En la Tabla 2.1.4.1, se puede apreciar que la metodología, estándares y marco de trabajo analizados, cubren el proceso de análisis y gestión de riesgos; la diferencia radica en el tipo de acceso que se tiene a la documentación, algunas son de acceso público y otras restringido para miembros de las entidades promotoras o de pago directo. Además, se cuenta con versiones actualizadas por sus creadores, entidades reconocidas a nivel mundial, lo que da un respaldo importante a cada una de ellas.

Metodología/Estándar	Creador	Fecha última versión	País	Ámbito	Acceso
OCTAVE Operationally Critical Threat, Asset, and Vulnerability Evaluation	CERT - Coordination Center del Software Engineering Institute de la Universidad Carnegie Mellon	2005	Estados Unidos	Método de análisis y gestión de riesgos orientado a Activos.	Público
NTE INEN-ISO/IEC 27005:2012	ISO - Organización Internacional para la Estandarización	2013		Estándar para la gestión del riesgo de seguridad de la información.	Restringido / de pago
COBIT - Control Objectives for Information and Related Technology	ISACA – Information Systems Audit and Control Association	2012		Marco de trabajo de control interno para TI, que ofrece una serie de mejores prácticas, las cuales están orientadas al control de la información y tecnología relacionada	Restringido / de pago

Tabla 2.1.4.1: Metodologías gestión de riesgo – Origen

En la Tabla 2.1.4.2, se evidencia que las etapas, faces o procesos guardan cierta similitud y enfoque estructurado, ya que todas separan las actividades de análisis de riesgos frente a la gestión de riesgos; las diferencias entre una y otra, radica en el desarrollo particular de cada etapa o fase.

Metodología / Estándar	Ámbito de aplicación	Etapas / Fases que se llevan a cabo
OCTAVE Operationally Critical Threat, Asset, and Vulnerability Evaluation	Cualquier organización pública o privada.	Fase 1- Construir perfiles de amenazas basados en los activos Proceso 1: Identificar el conocimiento de los altos directivos Proceso 2: Identificar el conocimiento de los directivos de áreas operativas Proceso 3: Identificar el conocimiento del personal operativo Proceso 4: Crear perfiles de amenaza Fase 2- Identificar vulnerabilidades en la infraestructura Proceso 5: Identificar componentes claves Proceso 6: Evaluación de componentes seleccionados Fase 3- Desarrollar estrategias y planes de seguridad Proceso 7: Realizar un análisis de riesgos Proceso 8: Desarrollar estrategias de protección
NTE INEN-ISO/IEC 27005:2012	Orientada a los sistemas informáticos	1. Establecimiento del contexto 2. Valoración del riesgo 3. Tratamiento del riesgo 4. Aceptación del riesgo 5. Comunicación del riesgo 6. Monitoreo y Revisión
COBIT - Control Objectives for Information and Related Technology	Cualquier organización pública o privada.	1 Proceso del Dominio de Gobierno EDM03. 1 Proceso del Dominio de Gestión APO12.

Tabla 2.1.4.2: Metodologías gestión de riesgo – Alcance y Etapas

Las comparativas siguientes, consideran otros parámetros de análisis como: alcance, tipo de análisis, tipo de riesgo, elementos constitutivos, objetivos de seguridad, inventario y herramientas para implementación que disponen. Comparativas adaptadas del trabajo “Análisis De Riesgos De Seguridad De La Información” [39], cuyos valores de cuantificación están dados por: ① No tiene; ② Pobre; ③ Satisfactorio; ④ Amplio; ⑤ Completo

NOMBRE	ALCANCE CONSIDERADO	
	ANÁLISIS DE RIESGOS	***GESTIÓN DE RIESGOS***
ISO 27005:2012	⑤	⑤
OCTAVE	⑤	⑤
COBIT	⑤	⑤

Tabla 2.1.4.3: Metodologías gestión de riesgo – Alcance

NOMBRE	TIPO DE ANÁLISIS		
	Cuantitativo	*Cualitativo*	*Mixto*
ISO 27005:2012	③	⑤	③
OCTAVE	③	③	③
COBIT	⑤	⑤	⑤

Tabla 2.1.4.4: Metodologías gestión de riesgo – Tipo de Análisis

NOMBRE	TIPO DE RIESGO		
	Intrínseco	*Efectivo*	*Residual*
ISO 27005:2012	①	⑤	②
OCTAVE	①	⑤	②
COBIT	①	⑤	②

Tabla 2.1.4.5: Metodologías gestión de riesgo – Tipo de Riesgo

NOMBRE	ELEMENTOS DEL MODELO						
	Procesos	*Activos*	*Recursos*	*Dependencias*	*Vulnerabilidades*	*Amenazas*	*Salvaguardas*
ISO 27005:2012	①	⑤	⑤	⑤	⑤	⑤	⑤
OCTAVE	⑤	⑤	⑤	⑤	⑤	⑤	⑤
COBIT	⑤	⑤	⑤	⑤	⑤	⑤	⑤

Tabla 2.1.4.6: Metodologías gestión de riesgo – Componentes

NOMBRE	OBJETIVOS DE SEGURIDAD					
	Confidencialidad	*Integridad*	*Disponibilidad*	*Autenticidad*	*Trazabilidad*	*Otros*
ISO 27005:2012	⑤	⑤	⑤	⑤	⑤	Fiabilidad
OCTAVE	⑤	⑤	⑤	①	①	①
COBIT	⑤	⑤	⑤	⑤	⑤	①

Tabla 2.1.4.7: Metodologías gestión de riesgo – Objetivos de Seguridad

NOMBRE	INVENTARIOS				
	Tipos de recursos	*Vulnerabilidades*	*Amenazas*	*Salvaguardas*	*Otros*
ISO 27005:2012	⑤	⑤	⑤	⑤	Criterios de valoración de activos. Restricciones para la reducción del riesgo
OCTAVE	⑤	⑤	⑤	⑤	①
COBIT	⑤	⑤	⑤	⑤	①

Tabla 2.1.4.8: Metodologías gestión de riesgo – Inventarios

NOMBRE	AYUDAS A LA IMPLANTACIÓN					
	Herramienta	*Plan de proyecto*	*Técnicas*	*Roles*	*Comparativas*	*Otros*
ISO 27005:2012	①	②	①	②	①	①
OCTAVE	①	⑤	⑤	⑤	①	Cuestionarios
COBIT	⑤	⑤	⑤	⑤	⑤	①

Tabla 2.1.4.9: Metodologías gestión de riesgo – Herramientas.

2.2 DISEÑO DE UNA ESTRATEGIA DE INTEGRACIÓN DE ESTÁNDARES Y BUENAS PRÁCTICAS DE GESTIÓN DE RIESGOS DE SERVICIOS DE CLOUD COMPUTING BASADOS EN COBIT, OCTAVE E ISO27000

Una vez que en el numeral 2.1, se analizó y justificó el estándar, la metodología y el marco de trabajo a emplearse en el desarrollo del *Modelo de Gestión de Riesgos de Infraestructura como Servicios (IaaS) de Cloud Computing aplicado a entidades del sector público ecuatoriano*, mismo que se resume en la Tabla 2.2.1,es necesario establecer una estrategia de integración, semejante al mostrado en la Figura 2.1.4.1, donde, a partir del modelo básico de gestión de riesgos [40], el marco de trabajo COBIT permita la integración o mapeo de su dominios, con las fases de la metodología OCTAVE y con los proceso de la norma ISO/IEC 27000,

COBIT	ISO27005	OCTAVE
• Cubre el gobierno de los riesgos (EDM) • Define un proceso global de gestión de riesgos • Es prescriptivo ya que permite personalizar, pero implica mayor tiempo y habilidad. • Tiempos Ramp-up más largos que OCTAVE. • Integra al gobierno de TI en el gobierno Corporativo, equilibrando entre la obtención de beneficios y la optimización de los niveles de riesgo. • Separa Gobierno y Gestión ya que abarcan y sirven propósitos diferentes. • Alinea los objetivos de TI con los objetivos del negocio. • Marco de facto para todo el control de TI.	• No cubre el gobierno de los riesgos. • Se centra en la evaluación de los riesgos de seguridad de la información usando los controles de la ISO27002. • Provee directrices para la gestión de riesgos, pero no ofrece metodología alguna para la gestión de riesgos corresponde a la organización definirlo, es decir, establece el ¿Qué?, pero no el ¿cómo? • Riesgos basado en amenazas/vulnerabilidades y basado en escenarios de riesgo. • Iterativo o mejora continua (Plan/Do/Check/)	• No cubre el gobierno de los riesgos. • Ayuda a la gestión de riesgos de seguridad de la información al igual que la ISO • No es prescriptivo y por tanto los tiempos de Ramp-up son más cortos. • Proporciona material y herramientas como hojas de cálculo para apoyar el proceso. • Se ajusta dentro del tiempo y la disponibilidad del recurso humano, del presente proyecto. • Es cualitativo lo que reduce el tiempo de análisis. • No explica en forma clara la definición y determinación de los activos de información • Facilita la creación de metodologías de análisis de riesgo • Cualquier metodología que aplique los criterios definidos por OCTAVE puede considerarse compatible.

• Evaluación integral de TI.		• Iterativo una vez implementadas las salvaguardias. • Establecen los principios fundamentales y los atributos de gestión de riesgos

Tabla 2.2.1: Justificación uso de COBIT, OCTAVE e ISO27005.

Integración o mapeo de los procesos, fases y dominios, sintetizados en la Tabla 2.1.4.2, donde se puede evidenciar que los controles de COBIT son aún más amplios que la ISO/IEC 27000 ya que integra al gobierno de TI con el gobierno Corporativo; mientras que la metodología OCTAVE, aplica las directrices para la gestión de riesgos establecidas por la ISO/IEC27000.

PROPUESTA MODELO DE GESTIÓN DEL RIESGO			COBIT	ISO/IEC27005			OCTAVE
GOBIERNO DE NUBE	**Evaluar la necesidad**		**EDM03.01** Evaluar la gestión del riesgo				
	Metas/Objetivos Organizacionales y de TI		**EDM03.02** Orientar la gestión de riesgo				
	Estructura Organizativa		**EDM03.03** Supervisar la gestión del riesgo				
CONSIDERACIONES A LA NUBE	**Proceso de Negocio**			Establecimiento del contexto			
	Modelo de Servicio						
	Modelo de Despliegue						
	Proveedor de Nube						
GESTIÓN DEL RIESGO	**Valoración**	**Identificación**	**APO12.01** Recolectar datos	Valoración	Análisis	Identificación	**Fase1**: Construcción de los perfiles de amenazas basados en activos
		Análisis	**APO12.02** Analizar riesgos			Estimación	**Fase2**: Identificación de la infraestructura de vulnerabilidades
		Evaluación			Evaluación		
	Tratamiento	**Evitar**	**APO12.03** Mantener perfil del riesgo	Tratamiento			**Fase3**: Estrategia y desarrollo del plan
		Reducir	**APO12.04** Expresar el riesgo				
		Transferir	**APO12.05** Definir un portafolio de acciones para la gestión de riesgos				
		Conservar	**APO12.06** Responder al riesgo				
	Aceptación riesgo residual.			Aceptación			
	Comunicar y monitorear.			Comunicación			
				Monitoreo y revisión			

Tabla 2.1.4.2: Mapeo procesos COBIT, ISO27005 y OCTAVE.

Propuesta metodológica que se encuentra adaptada a las necesidades de la Organización Caso de Estudio, tratando de cumplir las siguientes características:

- Alineada y basada en normas y metodologías para la gestión de riesgos aceptadas mundialmente.
- Enfoque holístico y sistémico hacia el riesgo al identificar todos los elementos interrelacionados que son requeridos.
- Enfoque cualitativo y conformación de equipos mixtos durante su implantación.
- Enfocada a procesos de negocios y soporte a la organización.
- Distinción entre el gobierno del riesgo y las actividades de la gestión de riesgos.
- Adaptable y objetiva a cualquier entorno.

Metodología de Gestión de Riesgos integrada por un conjunto de procesos y actividades, los cuales están claramente identificadas en tres fases o dominios: el Gobierno de Nube, las Consideraciones hacia la Nube y la Gestión de Riesgos de Nube.

Donde, el principal objetivo del Gobierno de Nube es asegurar la optimización del riesgo mediante el entendimiento, la articulación y la comunicación del apetito y la tolerancia al riesgo a todo nivel organizacional; mientras que el principal objetivo de las Consideraciones de Nube es proveer tanto a nivel directivo como operativo un conjunto de pautas para el cumplimiento normativo, localización y seguridad de los activos de información a ir a la Nube; finalmente, el principal objetivo de la Gestión de Riesgos es identificar, evaluar y reducir el riesgo relacionado con la Nube, dentro de los niveles de tolerancia establecidos por el Gobierno de Nube. Objetivos que serán desarrollados en mayor detalle en las siguientes etapas del modelo propuesto.

Es preciso indicar que, al igual que la diversidad de normas, metodologías y marcos de trabajo para la gestión de riesgos, existe un sin número de trabajos investigativos a nivel académico que desarrollan modelos de gestión de riesgos para la seguridad de la información mediante la integración o mapeo de los primeros. Trabajos que proveen una visión clara y sirven como referente durante el diseño de la estrategia de integración del presente trabajo.

2.2.1 FILOSOFÍA DEL MODELO

La filosofía del modelo proporciona un marco conceptual para el desarrollo del Modelo de Gestión de Riesgos de Infraestructura como Servicios (IaaS) de Cloud Computing aplicado a entidades del sector público ecuatoriano, basado en marcos de trabajos, normas y buenas prácticas mundialmente aceptadas, pero adaptadas a la normativa vigente del estado ecuatoriano, a fin de proveer a nivel directivo y operativo de TI, una guía detallada para la adopción y gestión de riesgos de servicios de Nube.

Como toda buena metodología, definir los objetivos y líneas de acción por adelantado aumenta las posibilidades de éxito. En consecuencia, un plan bien desarrollado que defina claramente los objetivos de la organización y las características específicas del papel de la Computación en la Nube, previamente analizadas en el numeral 1.1, permitirá una gestión acertada para la toma de decisiones. Entre los requisitos previos a considerarse durante una evaluación o proceso de adopción de la Computación en la Nube, se tiene: un modelo de gobernanza bien definido, una estructura de información eficaz, una comprensión exacta de habilidades internas de TI y un apetito de riesgo bien establecido. Sin embargo, la mayoría de organizaciones consideran a la evaluación de riesgos y a los programas de gobernanza como opcionales, por lo tanto, no es nada raro que adopten soluciones en la Nube sin aplicar una evaluación formal de riesgos o esfuerzo alguno por ajustar su Gestión Integral de Riesgos (ERM) o programa de gobernanza. Es una buena práctica incorporar la Gobernanza de Nube en las etapas iniciales antes de que se adopte una solución en la nube. Para aquellas organizaciones que ya optaron por la Computación en la Nube sin aplicar las mejores prácticas de Gestión de Riesgos Institucional, todavía es prudente realizar una evaluación de riesgos y establecer una Gobernanza de Nube.

El nivel de ajuste requerido para un programa ERM existente en la organización que pretende optar por la Computación en Nube depende de muchos factores, tales como: los procesos de negocio, el modelo de despliegue, el modelo de servicio, la naturaleza de los riesgos asociados al CSP y el entorno de control organizacional. En todo caso, será responsabilidad de la Alta Directiva determinar el Apetito de Riesgo que está dispuesto a tolerar de todo el universo de posibles eventos

asociados a una solución en la Nube, dado que algunos de estos eventos se extienden más allá de las fronteras tradicionales de la organización, e incluyen algunos eventos que tienen un impacto sobre el CSP y que soporta a la organización.

Si bien la adopción de la Computación en la Nube podría ser un cambio importante para una organización, la Alta Directiva puede utilizar un marco de trabajo de Gestión Integral de Riesgos (ERM) probado para evaluar y gestionar eficazmente los riesgos relacionados durante todo su ciclo de vida. En la Figura 2.2.1.1, se muestra el marco de trabajo propuesto, adaptado del "Committee of Sponsoring Organizations of the Treadway Commission (COSO)", y del mapeo de los procesos, fases y actividades para la gestión de riesgos provistas por la norma ISO/IEC 27005:2012, la metodología OCTAVE y el marco de trabajo COBIT, constituyéndose en la base referencial sobre la que se ha establecido el presente modelo, el cual está dirigido a los profesionales de seguridad y redes de TI y a la alta directiva organizacional.

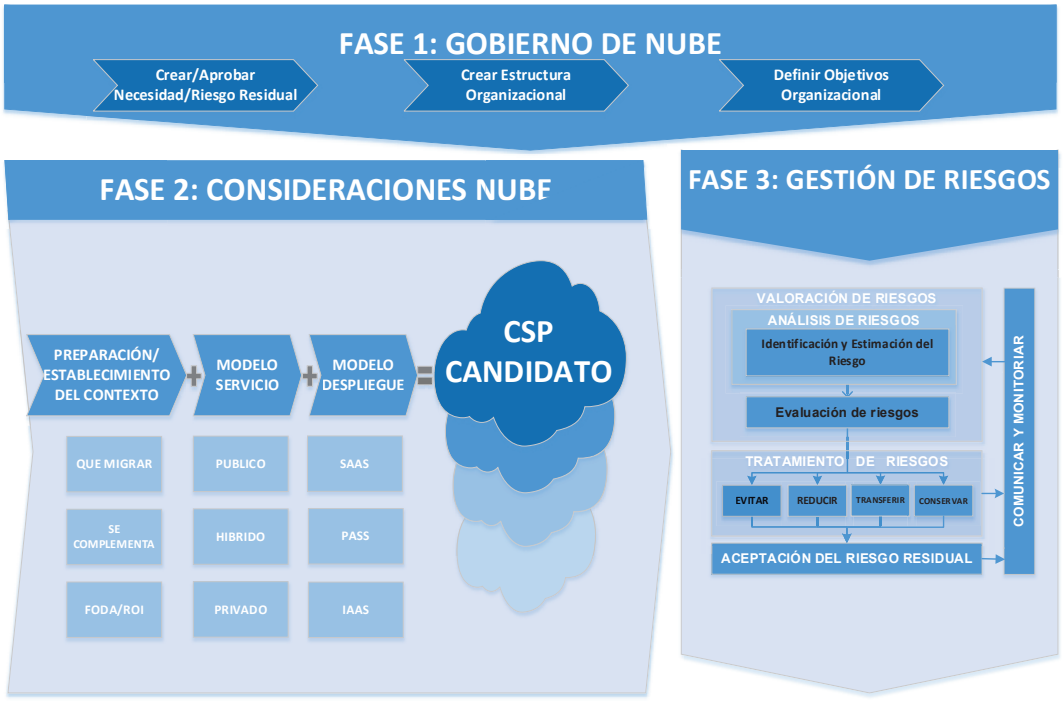

Figura 2.2.1.1 Marco de Trabajo para la Gestión de Riesgos en la Nube

2.2.2 DESCRIPCIÓN DE LA METODOLOGÍA

De acuerdo a la Figura 2.2.1.1, el modelo propuesto para la Gestión de Riesgos de Infraestructura como Servicios (IaaS) de Cloud Computing aplicado a entidades del sector público ecuatoriano se compone de tres fases, todas interrelacionadas entre sí, de tal forma de que se pueda retornar entre ellas a fin de incorporar variables no consideradas o no conocidas, garantizando la mejora continua, tan común en la mayoría de normas como la ISO.

La metodología comienza por proponer un modelo sencillo que sirva de apoyo a los responsables de la toma de decisión frente a la necesidad de adoptar la Computación en la Nube, considerando aspectos iniciales, operativos, jurídicos y de gestión de riesgos como guías para la identificación de la solución, que mejor se adapte a las necesidades de la organización.

La siguiente fase abarca todas aquellas consideraciones que cualquier organización que este por incorporar una solución de Computación en la Nube debe tener en cuenta, mismas que deben ser puestas en consideración de la Alta Directiva para su aprobación como un primer entregable del modelo propuesto. Entre las consideraciones a tener en cuenta se destacan aspectos técnicos, financieros, legales, normativos, contractuales, modelos de despliegue y/o servicios, mismos que deben estar alineados y ajustados al modelo o sistema de Gestión de Riesgos Organizacional (ERM) y al Apetito de Riesgo establecido por la Alta Directiva. Cabe indicar que para el presente trabajo por modelo de despliegue, se referirá a cualquier de las tres siguientes opciones: Nube Pública, Nube Privada o Nube Comunitaria; cada una respaldadas por los modelos de servicios: IaaS, PaaS y SaaS; Sin considerar soluciones hibridas, ya que supone un mayor grado de complejidad puesto que combina el uso de distintos modelos de despliegue y/o servicios.

La última fase, se enfoca en proporcionar un marco de trabajo para gestionar y mitigar eficazmente los riesgos relacionados a la Computación en Nube. Riesgos previamente identificados por reconocidas organizaciones internacionales pero acopladas al entorno nacional. Al igual que la fase anterior, dicho marco de trabajo debe estar en concordancia con el modelo de gestión de riesgo organizacional, con

la normativa legal vigente y con las demás normas, estándares, metodologías y marcos de trabajos mundialmente aceptados para la gestión de riesgos.

2.2.3 DESARROLLO DEL MODELO

El desarrollo del Modelo de Gestión de Riesgos de Infraestructura como Servicios (IaaS) de Cloud Computing aplicado a entidades del sector público ecuatoriano busca ser un instrumento útil y sencillo, cuyos resultados o entregables de cada fase deben ser puesto a consideración del Consejo Directivo para sopesar el ahorro en costos y otros aspectos atractivos como la flexibilidad y la agilidad, contra los temas críticos inherentes con la seguridad, la gestión del riesgo, el cumplimiento normativo y otros temas que pudiesen traer implicancias a la entidad gubernamental caso de estudio. No obstante, no constituye una metodología mandataria, pues corresponde a cada organización ajustarle a su propio enfoque de gestión de riesgos de acuerdo a su propio contexto y objetivos específicos.

El Modelo de Gestión de Riesgos propuesto, no solo está destinado a potenciales usuarios de la Computación de Nube – Instituciones de la Administración Pública Central, Dependiente e Institucional – sino a cualquier persona natural o jurídica, entidad pública o privada, interesadas en definir estrategias para la gestión de riesgos en la nube y obtener una base que les permita analizar, si lo tuviesen, su actual despliegue de nube pero desde el punto de vista de gestión de riesgos, de esta manera acompañarlos en la elaboración o replanteo de sus requisitos de seguridad de la información de nube que deberían ser plasmados en el respectivo instrumento legal, contrato y/o acuerdos de nivel de servicio (SLA), es decir, sirve como guía pre-contractual, y puede utilizarse a lo largo de todo el ciclo de adopción de Nube.

El modelo propuesto para cada fase ofrece un conjunto de posibles variables y/o requisitos a tenerse en cuenta, la ausencia o incumplimiento de uno o más de estos acarreará la no idoneidad del modelo y/o servicio requerido para satisfacer las expectativas de los usuarios.

Cabe indicar que en el desarrollo de cada fase existirán ciertos criterios, variable o requisitos que no serán descritos muy detalladamente o simplemente serán enunciados.

2.2.3.1 Fase I: Gobierno de Nube

El gobierno de Nube por ser una actividad de alto nivel de gestión tiene la autoridad para tomar decisiones, crear transparencia organizativa, determinar la responsabilidad por las acciones y los resultados, y proporcionar herramientas que garanticen que los procesos, políticas, normativa y resoluciones se sigan a todo nivel organizacional. El gobierno de Nube al ser el conjunto de procesos que asegura el uso eficaz y eficiente de la Computación en Nube, en la consecución de los objetivos estratégicos de la organización se encuentra presente en todo el ciclo de vida del modelo de gestión de riesgos propuesto y esquematizado en la Figura 2.2.1.1.

El Gobierno de Nube asegura que se evalúen las necesidades y condiciones de las partes interesadas de forma equilibrada y priorizada, supervisando el desempeño, cumplimiento y avance respecto a la dirección y objetivos acordados en la gestión de riesgos [34].

Entre las actividades que se debe realizar en esta fase se tiene:

- Establecer la necesidad de nube como punto de partida de la primera iteración del modelo propuesto. Para las siguientes iteraciones será la de aceptar o no el riesgo residual.
- Definir objetivos y/o metas organizacionales.
- Identificar e implementar la estructura organizativa apropiada (matriz RACI) y
- Analizar y aprobar continuamente los entregables de cada una de las fases.

2.2.3.2 Fase II: Consideraciones hacia la Nube

Sin duda la computación en nube ofrece diversidad de ventajas, analizadas en los numerales 1.1.5 y 1.1.6, pero ¿cómo saber si la organización caso de estudio, desde el punto de vista de la gestión de riesgos, se encuentra lista para adoptar y/o migrar a la nube? Actualmente, existe diversidad de consideraciones organizacionales y tecnológicas que tienen un efecto profundo sobre el conjunto de iniciativas de camino a la nube, pero ninguna normada, peor aún que se maneje desde la perspectiva del riesgo. Al no existir una guía normada de camino a la nube, se constituye en responsabilidad de cada organización establecer una; cuya

complejidad dependerán de factores endógenos a la organización y de aspectos como el nivel de seguridad deseado, los requisitos legales o contractuales respecto a la soberanía de la información, entre otros.

Por lo tanto, la decisión de migrar a la nube no se debería tomar a la ligera, ya que afecta a muchas áreas del negocio y requiere de un cambio importante en los métodos tradicionales y sus procesos. Por lo que las organizaciones deben: tener una visión clara de lo que quieren lograr con dicha migración en términos de sus objetivos organizacionales; entender los riesgos e implicaciones para la organización en conjunto, no solo con lo relacionado con lo económico o tecnológico; incluir el diseño de medidas y estrategias de mitigación adecuadas para manejar los riesgos y retos asociados. Consideraciones que a la postre ayudaran al nivel directivo y de TI a identificar un modelo de nube que mejor satisfaga las necesidades de la organización,

Por lo expuesto, en esta sección se ofrece una guía práctica para ayudar a aquellas organizaciones a establecer si ¿Están listos para ir a la nube? y ¿Qué activos de información deben ir a la nube?, si es así, ¿Qué modelo de servicio? o ¿Qué modelo de despliegue es el más viable? y ¿Sé ajusta a las necesidades del negocio? Para finalmente determinar el Proveedor de Servicio en la Nube (CSP) que satisfaga los anteriores planteamientos. Guía de Camino a la Nube, que se esquematiza en la Figura 2.2.3.1, y que sintetiza iniciativas, estudios, mejores prácticas, normas, controles y métricas de cumplimiento establecidas en la industria para proporcionar información y directrices para todos los usuarios de la nube, incluyendo auditores, usuarios finales e implementadores de soluciones, con el fin de que todos puedan evaluar soluciones de nube privadas y/o públicas, de infraestructura, plataforma o software como servicio, previo a su implantación.

Figura 2.2.3.1 Consideraciones hacia la Computación a la Nube

Una de esas iniciativas es el “Consensus Assessments Initiative Questionnaire – CAIQ [41]” de la Cloud Security Alliance (CSA), cuestionario gratuito basado en estándares (ISO 27001) y las mejores prácticas de la industria (COBIT5) que ofrece a los clientes de soluciones en la Nube una visión transparente de las medidas de seguridad implementadas por proveedores de nube, quiénes deben llevar a cabo procedimientos y procesos de seguridad para cumplir con las mejores prácticas. Este cuestionario incluye un conjunto de más de 140 preguntas, adaptadas al caso de estudio en el ANEXO 2, que un consumidor y/o auditor de nube debería plantear al proveedor de nube candidato, a fin de responder a preguntas como:

Organizacional:

- ¿Su estrategia de integración a la nube está alineada con el apetito de riesgo organizacional?
- ¿Su organización cuenta con el personal, habilidades y nivel de experiencia adecuados para lograr un cambio exitoso a la nube?
- ¿El equipo de gestión ha considerado en su planificación de Nube, qué inversiones de TI podrían perderse?

Tecnología:

- ¿Se le han realizado pruebas a la infraestructura y arquitectura de TI y de seguridad de su organización para verificar si es compatible con la nube?
- ¿La red de su organización tiene la capacidad para soportar tráfico de red adicional debido al acceso de las aplicaciones a través de internet?

Seguridad y privacidad:

- ¿Se ha realizado una evaluación del impacto al negocio para los servicios que se cambiarán a la nube para sustentar la planeación de continuidad del negocio y la recuperación de desastres?
- ¿Su organización cuenta con protocolos de autenticación seguros para los consumidores que trabajan en la nube? ¿Cómo gestionar el acceso a datos para usuarios privilegiados? ¿Cómo proteger la información de la organización contra el abuso de usuario?

- ¿Cómo gestionar la seguridad de la información de la organización? ¿Cuáles son los diferentes riesgos involucrados? ¿Cómo proteger el servicio contra las amenazas de Internet?

Legal, gobierno corporativo, cumplimiento y auditoría:

- ¿La alta directiva ha sopesado el valor y los costos de oportunidad que respalden la misión de la organización? ¿El equipo de gestión tienen estrategias para medir y dar seguimiento al valor del rendimiento de la inversión en la nube en relación con el riesgo?
- ¿La organización ha tomado en cuenta todos los requisitos relacionados con el flujo transfronterizo de información? ¿Dónde se encuentran los datos de la organización?
- ¿Su organización ha definido criterios mínimos para la cancelación de los servicios (incluyendo datos, devolución de activos, privacidad de datos, destrucción y migraciones) en los acuerdos contractuales?
- ¿Cómo monitorear y auditar las actividades? ¿Cómo la organización se asegura de que nadie ha manipulado sus datos?

Servicios:

- ¿Se ha realizado una revisión de due diligence del Proveedor de Servicios en la Nube para verificar que se pueden cumplir los requisitos de la organización? ¿Qué tipo de certificación o garantías se debe esperar del proveedor?
- ¿Su organización cuenta con procesos para mantener el cumplimiento reglamentario en áreas clave, como control de cambios entre las operaciones y servicios internos y basados en la nube?
- ¿Cuáles son las capacidades de recuperación de desastres del proveedor de nube? ¿Cuál es la disponibilidad esperada?

Respuestas que provee información importante para la evaluación de una posible solución en la Nube y poner en práctica una serie de acciones de mitigación y controles – numeral 2.3 – para reducir o eliminar las amenazas y/o riesgos

relacionadas con el servicio y modelo de entrega elegido, al tiempo de asegurar que los beneficios esperados de la migración a la Nube se materialicen.
En base a estas inquietudes, se plantea el siguiente enfoque para la valoración y determinación de la idoneidad de la organización desde el punto de vista de la gestión de riesgos para adoptar o migrar su infraestructura de TI a la nube con el menor impacto en el rendimiento y sin afectar la continuidad del negocio, a fin de alcanzar rápidamente los objetivos organizacionales:

- **Paso 1:** Preparación del medio interno.
- **Paso 2:** Selección del modelo de servicio en la nube
- **Paso 3:** Selección del modelo de despliegue en la nube
- **Paso 4:** Selección de proveedor de la nube

Sin embargo, el reto no termina después del paso 4. Incluso si la organización ha decidido ir a la nube basado en estos pasos y la confianza en el Proveedor de Servicios en la Nube, todavía hay una serie de inquietudes que deben ser solventadas por las siguientes fases del modelo propuesto.

2.2.3.2.1 Paso 1: Preparación del Medio Interno o Establecimiento del Contexto

Está claro que las iniciativas de la Computación en la Nube transforman el modelo de negocio tradicional y por lo tanto necesitan ser tratadas holísticamente, esto incluye a más de las consideraciones de gobierno y de gestión de riesgos, otros aspectos como, evaluación de las necesidades propias, las ventajas que se pueda obtener a partir del nuevo servicio, los posibles problemas que puedan surgir en el proceso y las medidas para reducir los riesgos. Aspectos a ser abordados en esta sección, a fin de ayudar a la organización a asegurar que sus iniciativas de nube no sólo aporten valor y cumpla los objetivos del negocio, sino también gestione los riesgos nuevos y potencialmente elevados:

- Identificar datos, aplicaciones o infraestructura a moverse a la nube.
- Validar que la infraestructura de TI se complementa y esté listo para moverse a la a la Nube
- Marco legal ecuatoriano aplicable

- Contrato y acuerdos de nivel de servicios (SLA)
- Identificar fortalezas, oportunidades, debilidades y amenazas relacionada con la Computación en la Nube, análisis FODA
- Desarrollar un marco de cálculo y evaluación del Retorno de la Inversión (ROI) en el ámbito de entidades del sector público ecuatoriano.
- Determinar qué inversiones de TI podrían perderse.

IDENTIFICAR LO QUE SE VA MOVER A LA NUBE (APLICACIONES, PLATAFORMA O INFRAESTRUCTURA)

Los procesos de migración o adopción de la nube deben ser progresivos y en transiciones controladas. Se recomienda seleccionar al inicio, datos, aplicaciones o infraestructuras de TI – activos de información – poco críticos, que permita desarrollar una experiencia piloto. Activos que deben estar clasificados de conformidad a normas o mejores prácticas existentes en el mercado, a fin de establecer la necesidad, las propiedades y el grado esperado de protección en lo referente a confidencialidad, integridad, disponibilidad y privacidad, mismos que dependerán en gran mediad del modelo de despliegue o del modelo de servicio seleccionado

VALIDAR QUE LA INFRAESTRUCTURA INTERNA DE TI SE COMPLEMENTA Y ESTÉ LISTO PARA LA COMPUTACIÓN EN LA NUBE.

Considerando que las soluciones de Nube requieren una visión estratégica a lo largo y ancho de la organización, es necesario dejar de lado el enfoque eminentemente táctico, de dar soluciones puntuales a problemas específicos, y habitualmente guiadas por la reducción de costes, ya que no solamente implica cambios a nivel tecnológico, sino también a nivel de recursos humanos y de procesos.

Un enfoque estratégico obliga a una centralización de recursos y conocimientos, dando mayor difusión al aprendizaje y estableciendo mayor colaboración entre las unidades de negocio y el departamento de TI, donde este último adquiere conocimiento sobre el negocio, no sólo para evitar que exista una desconexión respecto a lo que este demanda, sino para alcanzar un estado de identificación y generación de servicios conjuntos.

MARCO LEGAL LOCAL APLICABLE

Como se ha enfatizado, el cumplimiento normativo también es uno de los pilares de la seguridad en entornos de Nube. En este caso, el problema se presenta debido a la falta de transparencia de estas infraestructuras, por lo que es recomendable que el potencial usuario del servicio se informe claramente de cómo se gestiona el entorno por parte del proveedor del servicio, sin dejar de lado el cumplimiento de la normativa local.

Para las entidades de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva, una de las principales cuestiones legales es la soberanía y el control sobre la información que manejan, ya que son responsables del uso adecuado y de garantizar que sus obligaciones de protección de la información se extiendan a sus proveedores y a sus terceros, no debiendo ser la excepción los servicios de nube, donde el alojamiento de infraestructuras de nube puede ir más allá de la jurisdicción local.

Al respecto, la Secretaría Nacional de la Administración Pública – SNAP, mediante Acuerdo Ministerial 166, de septiembre de 2013, prohibió expresamente a las entidades de la Administración Pública la contratación, acceso y uso de servicios de Nube con empresas privadas o públicas cuyos centros de datos, redes, equipos, software base y de gestión, y cualquier elemento tecnológico necesario, se encuentren fuera del territorio nacional, más aún, si las condiciones de los servicios que tales empresas prestaren no se someten a la Constitución y Leyes Ecuatorianas [42]. Sin embargo, esto no quiere decir que la contratación de servicios de nube por parte de las entidades gubernamentales esté del todo vetada siempre y cuando se cumpla con los requisitos expuestos.

De acuerdo al “Análisis de los Riesgos Técnicos y Legales de la Seguridad en Cloud Computing” [17], a falta de una legislación exacta para Computación en la Nube, se puede utilizar normativas locales existentes, que cubran dichos vacíos, pero no con el alcance deseado que las soluciones de Nube demanda. En la Tabla 2.2.3.1, se resumen que aspectos de Nube al momento son cubiertos por estas normativas:

DERECHO NORMADO / LEY	Protección de datos	Confidencialidad y no divulgación	Propiedad intelectual	Limitación de responsabilidades	Indemnización	Garantías y compensaciones	Cambio de Control
Constitución de la República del Ecuador	X						
Ley del Sistema Nacional de registro de Datos Públicos		x					
Ley de comercio electrónico, firmas electrónicas y mensajes de datos	x	x					

Tabla 2.2.3.1: Cumplimiento normativo Local en Computación en la Nube

Evidenciándose que la protección de datos y la confidencialidad son las dos únicas áreas que al momento se encuentran protegidas, sin embargo, el resto de necesidades que demanda la Nube, no están siendo cubiertas por ninguna otra reglamentación. Lo que limita la adopción de la computación en la nube por parte del estado ecuatoriano.

CONTRATO Y ACUERDOS DE NIVEL DE SERVICIO (SLA)

El contrato al igual que los Acuerdos de Nivel de Servicio (SLA), se constituyen en el medio mediante el cual las entidades gubernamentales garantizan que sus obligaciones respecto a la soberanía y protección a la seguridad de la información se extiendan al proveedor de Nube y a sus terceros. Por lo tanto, a diferencia de los servicios tradicionales de internet e independientemente del modelo y/o tipo de servicio, el contrato debe ser el resultado de la negociación entre el cliente y el proveedor, en el que se especifique claramente los derechos y obligaciones de las partes.

No obstante, mientras la normativa ecuatoriana aborde las preocupaciones concretas en materia de seguridad y gestión de riesgos en la Nube, es responsabilidad de los departamentos: legal, contratación, TI y área requirente, establecer en el ámbito de su competencia las condiciones necesarias para abordar de manera efectiva los riesgos de seguridad, mediante el establecimiento de cláusulas contractuales relacionados con la disponibilidad, rendimiento, seguridad,

cumplimiento de las normas y privacidad, que el proveedor del servicio debe cumplir con respecto al servicio de Nube que va a proporcionar.

CALCULADO EL RETORNO DE LA INVERSIÓN (ROI)

Uno de los principales atractivos de la computación en la nube radica en que requiere un bajo costo inicial para generar un retorno sobre la inversión (ROI) rápido, perspectiva que considera únicamente los costos inmediatos de contratación, pero pasa por alto los costos a largo plazo de operación en la nube que podrían llegar a reducir al mínimo el retorno esperado, razón por la cual en ésta sección se tratará de establecer la base para cuantificar el valor del retorno e identificar todos los costos potenciales, considerando la perspectiva a corto, mediano y largo plazo, los costos de terminación y beneficios tangible e intangibles, al momento de sopesar la decisión de proceder o no con una solución en la nube por parte de entidades del sector publico ecuatoriano.

ANÁLISIS FORTALEZAS OPORTUNIDADES DEBILIDADES Y AMENAZAS (FODA)

El análisis de Fortalezas, Oportunidades, Debilidades y Amenazas, es otra consideración que cualquier potencial usuario de Nube debe tener en cuenta como acción inicial y mínima a llevar a cabo, en especial la administración pública ecuatoriana que en los últimos años ha realizado ingentes inversiones en tecnologías de la información y comunicación.

Por esta razón, una vez que a nivel directivo se ha identificado la necesidad de incorporar la Computación en la Nube como estrategia de TI a corto, mediano o largo plazo para determinada aplicación, plataforma o infraestructura, es necesario identificar sus puntos positivos y negativos adaptados a la realidad del sector publico ecuatoriano.

Análisis FODA que integre los aspectos más relevantes a considerarse durante todo el ciclo de adopción de la computación en la nube por parte del sector público ecuatoriano, ya que da a conocer la situación real a la que estaría expuesto.

2.2.3.2.2 Paso 2: Selección del Modelo de Servicio en la Nube

En la sección 1.1, se analizó los diferentes modelos de servicios que provee la Computación en la Nube: IaaS, PaaS o SaaS; cada uno con sus características y

atributos únicos para ahorrar tiempo, dinero y operar más eficientemente, sin embargo, también disponen de inhibidores, amenazas o riesgos, analizados en la sección 1.2, que varían desde la perspectiva de la protección de secretos comerciales críticos para el negocio (seguridad), al cumplimiento con los requisitos legales y la protección de datos personales (cumplimientos normativo), entre otros. Por lo tanto, la Computación en la Nube abarca varias opciones de implementación, cada una con un perfil de seguridad y confianza diferente. Por eso, la pregunta no es si ¿se debe confiar en "la nube"?, sino ¿qué solución de nube (si la hubiera) se alínea con objetivos estratégicos de la organización y de las partes interesadas? Frente a esta interrogante ISACA propone el siguiente árbol de decisión [26] para la elección del modelo de servicios en la nube y que se esquematiza en la Figura 2.2.3.3, cuyo análisis detallado se describe en la Tabla 2.2.3.3.

Según la Figura 2.2.3.2, y los reportes "Cloud Computing Information Assurance Framework [43]" y "Cloud Computing Security Reference Architecture [10]", de la ENISA y NIST respectivamente, en una IaaS, la organización no administra o controla la infraestructura de nube subyacente, pero tiene control sobre los sistemas operativos, almacenamiento, aplicaciones implementadas y posiblemente control limitado sobre ciertos componentes de red; Mientras en una PaaS, el usuario no administra o controla la infraestructura de nube subyacente incluyendo la red, servidores, sistemas operativos o el almacenamiento, pero tiene control sobre las aplicaciones desplegadas y posiblemente sobre la configuración para el entorno de aplicaciones; En el caso de una SaaS, el usuario no gestiona ni controla la infraestructura de nube subyacente incluyendo la red, servidores, sistemas operativos, almacenamiento o incluso capacidades de aplicación individuales, con la posible excepción de los ajustes de configuración de aplicaciones específicas de usuario limitadas. Por lo tanto, el modelo de servicio SaaS es, claramente, la solución que ofrece al cliente el menor grado de control directo sobre los parámetros de seguridad y resistencia, y que otorga un mayor grado de control y responsabilidad a los proveedores de los servicios de la nube. Por su parte, el IaaS es el que garantiza más capacidad de control directo, pero, al mismo tiempo, deja al cliente con toda la responsabilidad de implementar las medidas técnicas y procedimentales de seguridad y resistencia.

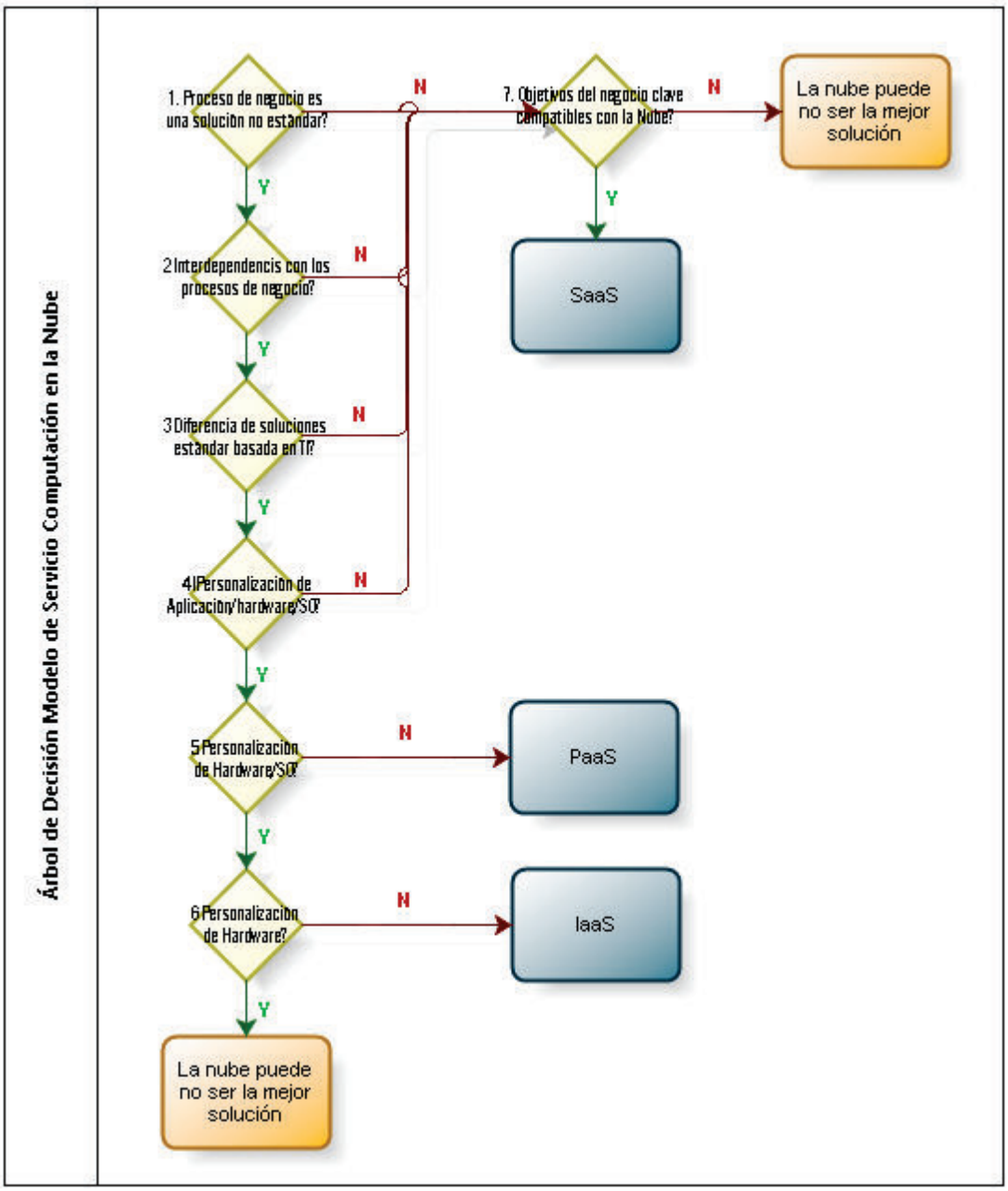

Figura 2.2.3.2 Árbol de decisión por Modelo de Servicio en la Nube

De ahí que, el árbol de decisión de la Figura 2.2.3.2, busca ayudar a la organización a determinar qué modelo de servicio satisface las necesidades del negocio, ya que puede conducir a una decisión de migrar a la nube o sugerir que la nube no es la mejor solución, según como se detalla en la siguiente Tabla 2.2.3.3.

Respuesta	Explicación	Siguiente Pregunta
1. ¿Es el proceso de negocio una solución no estándar?		
SI	Si el proceso de negocio utiliza soluciones no estándar, entonces se necesita analizar más afondo para determinar si el proceso de negocio es adecuado para una solución en la nube.	Pregunta 2: ¿Interdependencias con los procesos de negocio?
No	Si se usa una solución estándar, entonces la transición a la nube es relativamente fácil y los beneficios de adoptar una solución de nube serán muy probablemente alta.	Pregunta 7: ¿Objetivos del negocio clave compatibles con la Nube?
2. ¿Interdependencias con los procesos de negocio?		
SI	Si hay interdependencias con diferentes procesos de negocio, entonces, cualquier alteración de uno de estos procesos podría significar un cambio en la implementación de la aplicación en la nube.	Pregunta 3: ¿Diferencia de soluciones estándar basada en TI?
No	Si no hay interdependencias, entonces no será necesario introducir cambios. La solución de nube elegida será, por lo tanto, independiente.	Pregunta 7: ¿Objetivos del negocio clave compatibles con la Nube?
3. ¿Diferencia de soluciones estándar basada en TI?		
SI	Mientras la interdependencia puede implicar un cambio en la infraestructura de TI, no siempre es una necesidad. Si la interdependencia sí implica un cambio de este tipo, sin embargo, será necesario que la aplicación de nube sea cambiada. Este hecho influye en gran medida en la decisión de un modelo de servicios de nube. Por lo tanto, es importante delinear las diferencias entre la solución actual y la solución estándar proporcionada por un CSP.	Pregunta 4: ¿Personalización de Aplicación/hardware/SO?
No	Si no hay diferencias entre las soluciones de TI, entonces la oferta estándar del CSP se acoplarían a las necesidades del negocio.	Pregunta 7: ¿Objetivos del negocio clave compatibles con la Nube?
4. ¿Personalización de Aplicación/hardware/SO?		
SI	Una vez que se estableció que efectivamente existe una brecha entre las necesidades del negocio y las ofertas de servicio en la nube, es importante definir el nivel en que se encuentra dicha diferencia.	Pregunta 5: ¿Personalización de Hardware/SO?
No	Si la diferenciación se encuentra en la configuración de la aplicación estándar, entonces la oferta de nube cumplirá con las necesidades del negocio.	Pregunta 7: ¿Objetivos del negocio clave compatibles con la Nube?
5. ¿Personalización de Hardware/SO?		
SI	Después de establecer que la diferencia no está dentro de la aplicación, es importante establecer si la diferencia se encuentra a nivel de sistema operativo o de plataforma de hardware físico. La respuesta va a alterar la posibilidad de adaptación de nube.	Pregunta 6: ¿Personalización de Hardware?
No	Si la diferenciación se puede hacer a nivel de aplicación, no se necesita más profundización o análisis	Solución: PaaS
6. ¿Personalización de Hardware?		
SI	Después de establecer que la diferenciación se encuentra en el nivel físico, es muy poco probable una solución en la nube. Los CSPs están orientados hacia la estandarización dentro de su dominio; proporcionar hardware personalizado no es uno de sus	Solución: La computación en nube puede no ser la mejor solución para sus necesidades de negocio actuales.

	ofrendas típicas. Mientras que un CSP, sin duda, puede proporcionar plataformas de hardware personalizado, el alto costo y la relativa falta de experiencia en la plataforma personalizada del CSP eliminan la nube como una solución viable.	
No	Si la diferenciación se puede hacer en el nivel de sistema operativo, no se necesita más profundización o análisis.	Solución: IaaS
7. ¿Objetivos del negocio clave compatibles con la Nube?		
SI	Entre los objetivos del negocio clave que influyen en la decisión de optar por la nube se tiene: * Reducir a mediano y/o largo plazo el costo total de la propiedad (TCO). * Mejorar el flujo de caja por la disminución de las inversiones. * Pasar de los gastos de capital (CAPEX) a los gastos operativos (OPEX). * Mejorar la calidad de servicio (QoS) y / o SLAs. * Obtener acceso a la funcionalidad y / o experiencia en el campo.	Solución: SaaS
No	Si bien puede no haber restricciones técnicas para la adopción de la nube como una solución, es posible que los objetivos de negocio, de hecho, no sean compatible con la nube. La adopción de una solución en la nube requiere una visión a mediano y largo plazo. Por lo tanto, la nube no se puede utilizar como una solución para reducir los costos de inmediato.	Solución: La computación en nube puede no ser la mejor solución para sus necesidades de negocio actuales.

Tabla 2.2.3.2: Árbol de Decisión Modelo de Servicios de Computación en la Nube

2.2.3.2.3 Paso 3: Selección del Modelo de Despliegue en la Nube

Semejante al proceso de selección del modelo de servicio, en la Figura 2.2.3.3 se esquematiza el árbol de decisión para el establecimiento del modelo de despliegue en la nube, que pretende ayudar a la organización a determinar ir o no a la nube, este último, generalmente cuando los datos o el proceso es demasiado crítico o contiene datos tan sensibles para el negocio que el riesgo de ir a la nube sobrepasa los beneficios.

Según la Figura 2.2.3.3, una nube pública todavía enfrenta inquietudes, algunas de ellas se relacionan con la capacidad tecnológica del proveedor, la organización del cliente, el establecimiento e implementación de políticas, estándares y controles necesarios para tener ambientes de nubes verdaderamente confiables e interoperables. Los proveedores de nubes públicas no siempre pueden proporcionar la transparencia requerida por leyes y acuerdos de servicio relacionados con TI que suponen la ubicación física específica de los datos y otros recursos. Esto suele deberse a su renuencia a exponer sus operaciones en forma completa al escrutinio externo.

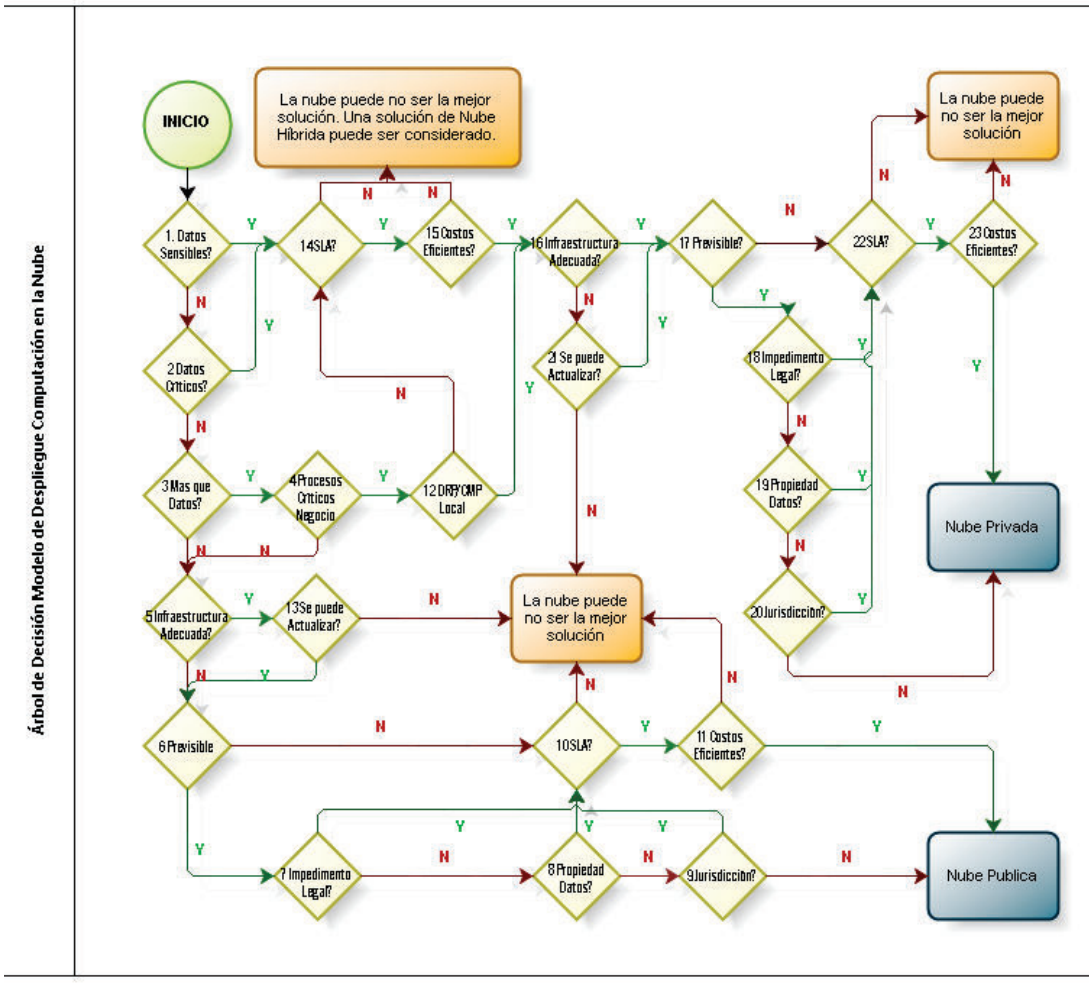

Figura 2.2.3.3 Árbol de decisión por Modelo de Despliegue en la Nube

Además, el mercado carece de agentes independientes y creíbles para examinar y certificar a proveedores de nubes públicas como adecuados para la información y las aplicaciones más confidenciales. Para organizaciones grandes como lo son las gubernamentales, que disponen de capacidad de escala y financiera para soluciones de negocio más sofisticadas, una solución de nube pública no es una opción convincente para aplicaciones de misión crítica o para las que procesan datos altamente confidenciales.

Para el caso de soluciones de nube privadas, estas enfrentan un conjunto más pequeño de desafíos de cumplimiento con normas, leyes y reglamentos en comparación con la nube pública porque la ubicación geográfica de los datos es clara y el control de los activos es directo. La organización puede adaptar los

procesos y procedimientos existentes a un ambiente más virtualizado y de autoservicio al mismo tiempo que mejora la transparencia y la capacidad de administración del ambiente computacional. Se debe tener presente que la implementación de nubes privadas puede realizarse fuera de las instalaciones con una nube privada externa. Esto se parece mucho a la subcontratación tradicional de data center dedicado, y puede ser tan seguro y se puede administrar tan de cerca como una nube privada en las instalaciones. Con una implementación sólida y las mejores prácticas operacionales, la nube privada puede ser más confiable y segura que la nube pública y la mayoría de los ambientes de TI actuales, ya que se puede crear más seguridad y más control granular sobre los datos y otros activos desde el principio. Así, las nubes privadas tienen la capacidad de proveer los beneficios de rendimiento y económicos de la nube de manera segura y protegida, facilitando la administración de la tecnología de la información y reduciendo el riesgo operacional.

Una solución de nube híbrida combina nubes públicas y privadas y permite a las organizaciones aprovechar los beneficios de ambas. El ambiente computacional más flexible y rentable de hoy en día incorpora una federación de nubes públicas y privadas, con las aplicaciones adecuadas ejecutándose en la nube pública; la mayoría de las aplicaciones de misión crítica y las que manejan información confidencial se ejecutan en una nube privada, y algunas aplicaciones se cruzan y usan servicios de nubes públicas y privadas. Consideraciones que son analizadas en la siguiente Tabla 2.2.3.3.

Respuesta	Explicación	Siguiente Pregunta
1. ¿Información sensible?		
Si	Al considerar moverse a una infraestructura de nube es muy importante estar consciente de cuáles son los datos que se moverán. Es imposible prever todos los riesgos y amenazas potenciales; Sin embargo, los datos de carácter sensible pueden ser colocados en la nube cuando los controles necesarios para protegerlos están en su lugar y trabajar con eficacia.	***Pregunta*** 14: ¿SLA?
No	Si los datos no son sensibles o si su carga a la nube no es requerida, entonces de los primeros pasos hacia la nube	***Pregunta*** 2: ¿Información Crítica?
2. ¿Información Crítica?		

Si	Los datos críticos pueden ser: • Planos • Fórmulas • Secretos comerciales • Cualquier información que sea absolutamente necesario para que la organización funcione Los datos críticos pueden ser colocados en la nube cuando los controles necesarios para protegerlos están en su lugar y funcionando con eficacia. Es importante señalar, sin embargo, que algunos de estos controles puede ser costoso y complejo, lo que puede aumentar el costo de trasladarse a la nube.	***Pregunta*** 14: ¿SLA?
No	Los datos no críticos se pueden colocar fácilmente en la nube.	***Pregunta*** 3: ¿Más que datos?
3. ¿Más que datos?		
Si	En casi todos los casos la decisión de trasladarse a la nube no se limita únicamente a los datos. Los datos en la nube a menudo son necesarios para ejecutar aplicaciones o como parte de los procesos de negocio.	***Pregunta*** 4: ¿Procesos de Negocios Críticos?
No	Si la decisión de trasladarse a la nube se limita únicamente a los datos, el siguiente paso es evaluar la disposición de la organización para este movimiento.	***Pregunta*** 5: ¿Infraestructura adecuada?
4. ¿Procesos de Negocios Críticos?		
Si	Para tomar una decisión correcta, es imprescindible determinar si los datos y las aplicaciones alojadas en la de nube soportan procesos críticos de negocio. Esta información le ayudará a determinar los requisitos que la solución en la nube debe satisfacer.	Pregunta 12: ¿DRP/BCM internos?
No	Cuando un proceso de negocio o aplicación de soporte no se considera crítico, puede ser más fácil moverse a la nube.	***Pregunta*** 5: ¿Infraestructura adecuada?
5. ¿Infraestructura adecuada?		
Si	Un movimiento hacia la nube es un paso hacia la reducción de la infraestructura informática de la organización; Sin embargo, se necesita una planificación adecuada antes de adoptar una solución en la nube. Algunas cosas a tener en cuenta como parte de la evaluación de la preparación incluyen: • Conectividad con el CSP (ancho de banda, la redundancia) • La seguridad de red (cifrado de datos durante la transferencia) • La integración entre los sistemas de nube y no nube • Conectividad de usuario (ancho de banda para el escritorio o dispositivos móviles)	***Pregunta*** 6: ¿Predecible?
No	Si se determina que la infraestructura actual de la organización no está preparado para integrarse con la nube, el siguiente paso es determinar si las necesidades del negocio son mayores que el costo de actualizar (análisis de viabilidad).	***Pregunta*** 13: ¿Se puede actualizar?
6. ¿Predecible?		
Si	Como parte de la evaluación preparatoria la organización debe determinar cómo funcionan y ejecutan/crecen/maduran los procesos de negocio. Esta información puede ayudar a anticipar la fluctuación de la capacidad (arriba o abajo) que deben ser parte del contrato con el CSP.	***Pregunta*** 7: ¿Impedimentos legales o de cumplimiento?
No	Cuando la organización no puede prever las fluctuaciones de capacidad, puede ser necesario un mayor análisis. La flexibilidad y la escalabilidad son dos características de la nube que la hacen más atractivo: un SLA flexible puede ser la solución hasta que la organización cuenta con requisitos más refinados.	***Pregunta*** 10: ¿SLA?
7. ¿Impedimentos legales o de cumplimiento?		
Si	Puede haber razones legales o de cumplimiento para qué los datos o ciertas funciones del negocio no puedan ser movidas a la nube. Es importante para el CSP implementar los controles necesarios para garantizar la continuidad jurídica y el cumplimiento de la organización. El CSP debe ser capaz de proporcionar la prueba de cumplimiento avalado por un organismo de auditoria o control independiente. La identificación de limitaciones legales o de cumplimiento deben ser abordados durante las negociaciones del contrato para estipular las expectativas de la organización y la forma en que serán satisfechas	***Pregunta*** 10: ¿SLA?

No	Si la organización no tiene ningún impedimento legal o de cumplimiento, los siguientes pasos para mover a la nube pueden ser abordados.	***Pregunta*** 8: ¿Propiedad de los datos?
8. ¿Propiedad de los datos?		
Si	El contrato con el CSP debe estipular claramente que la organización ES, y SEGUIRÁ SIENDO, el titular de los datos. Es igualmente importante que esta propiedad se mantenga a lo largo de todo el ciclo de vida de los datos. Por lo tanto, el contrato también debe describir los requisitos para disponer de los datos de forma adecuada cuando la organización a si lo considere. Si la propiedad de datos no se puede establecer correctamente, la organización puede optar por mover aquellos datos no sensibles y no críticos.	***Pregunta*** 10: ¿SLA?
No	Si la organización puede definir claramente la propiedad de los datos durante las negociaciones del contrato, los siguientes pasos para mover a la nube pueden ser abordados.	***Pregunta*** 9: ¿Jurisdicción?
9. ¿Jurisdicción?		
Si	A pesar de que la propiedad de los datos reside en la organización, las leyes locales e internacionales a menudo prohíben la transferencia o ciertos datos a los países que tienen leyes o reglamentos en conflicto. Por lo tanto, es importante para la organización conocer la ubicación de las instalaciones de almacenamiento de datos de la CSP y centros de procesamiento de datos para evitar infracciones legales. Es recomendable para la organización incluir en el contrato con el CSP las cláusulas necesarias que exijan al CSP limitar las ubicaciones de servicio a los aprobados por la organización.	***Pregunta*** 10: ¿SLA?
No	Si la organización no tiene limitación de la jurisdicción, la nube puede ser una solución adecuada.	***Solución***: ***Nube Publica***
10. ¿SLA?		
Si	La organización debe determinar de antemano los términos que serán incluidos en el SLA, considerando que los acuerdos estrictos o complejos podrían resultar en un mayor costo. Algunos de los términos que deben ser negociados y documentados en el SLA incluyen: • Disponibilidad • El tiempo de respuesta para las peticiones recursos de computación adicionales • Tiempo de respuesta de incidentes • Las políticas de copia de seguridad • Las políticas y procedimientos de retención y eliminación de datos • Gestión de Ruta • Los controles de seguridad • Recuperación y Continuidad objetivos • Controles para satisfacer los requisitos legales y de cumplimiento	***Pregunta*** 11: ¿Costo eficiente?
No	Si un SLA adecuada no puede ser acordado, trasladarse a la nube podría representar un nivel inaceptable de riesgo. Si el costo de la SLA es mayor que los beneficios del negocio, la solución de nube puede no ser la mejor solución.	***Solución***: La computación en nube puede no ser la mejor solución para sus necesidades de negocio actuales.
11. ¿Costo eficiente?		
Si	Dos de los principales objetivos de trasladarse a la nube constituye ser cada vez más rentable y ser capaz de reaccionar más rápida y económicamente a las situaciones cambiantes.	***Solución***: ***Nube Publica***
No	A menos que los beneficios del negocio sea mayor que el costo, una solución costosa puede no ser la opción correcta.	***Solución***: La computación en nube puede no ser la mejor solución para sus necesidades de negocio actuales.
12. ¿DRP/BCM interno?		

Si	Esta cuestión ya se puede abordar en el SLA, pero la organización aún debe estar dispuesto a considerar los planes adicionales de DR y BC. Un desastre dentro de la CSP es probable que cause un impacto en las operaciones de la organización. Por ejemplo, las rutas cambiarán y serán alterados los puntos de entrada, causando retrasos en las operaciones. Si un desastre tiene lugar dentro de la organización, mantener o re-establecer la conectividad con el CSP debe ser una parte fundamental de los esfuerzos de recuperación. Las organizaciones cuyos datos residen únicamente en la nube debe crear copias de seguridad a sus propias instalaciones para conservar las capacidades de recuperación y continuidad, incluso si el CSP está completamente fuera de línea	***Pregunta*** 16: ¿Infraestructura Adecuada?
No	Depender exclusivamente de las capacidades DRP/BCM del CSP puede exponer a la organización a interrupciones comerciales extendidas; sin embargo, si el costo de tener un DRP interno es mayor que los beneficios del negocio, la organización puede abordar esta cuestión de un modo más estricto en el SLA.	***Pregunta*** 14: ¿SLA?
13. ¿Se puede actualizar?		
Si	Si se determina que la infraestructura actual de la organización no está preparado para integrarse con la nube, el siguiente paso es determinar si las necesidades del negocio son mayores que el costo de actualizar (análisis de viabilidad).	***Pregunta*** 6: ¿Predecible?
No	Si el costo para mejorar la infraestructura actual es mayor que las necesidades del negocio, la nube no puede ser una solución todavía.	***Solución***: La computación en nube puede no ser la mejor solución para sus necesidades de negocio actuales.
14. ¿SLA?		
Si	La organización debe determinar de antemano los términos que serán incluidos en el SLA, considerando que acuerdos estrictos o complejos podrían resultar en un mayor costo. Algunos de los términos que deben ser negociados y documentados en el SLA incluyen: • Disponibilidad • El tiempo de respuesta para las peticiones recursos de computación adicionales • Tiempo de respuesta de incidentes • Las políticas de copia de seguridad • Las políticas y procedimientos de retención y eliminación de datos • Gestión de Ruta • Los controles de seguridad • Recuperación y Continuidad objetivos • Controles para satisfacer los requisitos legales y de cumplimiento	***Pregunta*** 15: ¿Costo eficiente?
No	Si un SLA adecuada no puede ser acordado, trasladarse a la nube podría representar un nivel inaceptable de riesgo. Si el costo de la SLA es mayor que los beneficios del negocio, la solución de nube puede no ser la mejor solución.	***Solución***: Nube completa puede no ser la mejor solución. Una solución de nube Hibrida puede ser considerada.
15. ¿Costo eficiente?		
Si	Dos de los principales objetivos de trasladarse a la nube constituye ser cada vez más rentable y ser capaz de reaccionar más rápida y económicamente a las situaciones cambiantes.	***Pregunta*** 16: ¿Infraestructura Adecuada?
No	A menos que los beneficios del negocio sea mayor que el costo, una solución cara puede no ser la opción correcta	***Solución***: Nube completa puede no ser la mejor solución. Una solución de nube Hibrida puede ser considerada.
16. ¿Infraestructura adecuada?		
Si	Un movimiento hacia la nube es un paso hacia la reducción de la infraestructura informática de la organización; Sin embargo, se necesita una planificación adecuada antes de adoptar una solución en la nube. Algunas cosas a tener en cuenta como parte de la evaluación de la preparación incluyen: • Conectividad con el CSP (ancho de banda, la redundancia) • La seguridad de red (cifrado de datos durante la transferencia) • La integración entre los sistemas de nube y no nube	***Pregunta*** 17: ¿Predecible?

	• Conectividad de usuario (ancho de banda para el escritorio o dispositivos móviles)	
No	Si se determina que la infraestructura actual de la organización no está preparado para integrarse con la nube, el siguiente paso es determinar si las necesidades del negocio son mayores que el costo de actualizar (análisis de viabilidad).	***Pregunta*** 21: ¿Se puede actualizar?
17. ¿Predecible?		
Si	Como parte de la evaluación preparatoria la organización debe determinar cómo funcionan y madurar los procesos de negocio. Esta información puede ayudar a anticipar la fluctuación de la capacidad (arriba o abajo) que deben ser parte del contrato con el CSP.	***Pregunta*** 18: ¿Impedimentos legales o de cumplimiento?
No	Cuando la organización no puede prever las fluctuaciones de capacidad, puede ser necesario un mayor análisis. La flexibilidad y la escalabilidad son dos características de la nube que la hacen más	***Pregunta*** 22: ¿SLA?
18. ¿Impedimentos legales o de cumplimiento?		
Si	Puede haber razones legales o de cumplimiento para qué los datos o ciertas funciones del negocio no puedan ser movidas a la nube. Es importante para el CSP implementar los controles necesarios para garantizar la continuidad jurídica y el cumplimiento de la organización. El CSP debe ser capaz de proporcionar la prueba de cumplimiento avalado por un organismo de auditoria o control independiente. La identificación de limitaciones legales o de cumplimiento deben ser abordados durante las negociaciones del contrato para estipular las expectativas de la organización y la forma en que serán satisfechas	***Pregunta*** 22: ¿SLA?
No	Si la organización no tiene ningún impedimento legal o de cumplimiento, los siguientes pasos para mover a la nube pueden ser abordados.	***Pregunta*** 19: ¿Propiedad de los datos?
19. ¿Propiedad de los datos?		
Si	El contrato con el CSP debe estipular claramente que la organización ES, y SEGUIRÁ SIENDO, el titular de los datos. Es igualmente importante que esta propiedad se mantenga a lo largo de todo el ciclo de vida de los datos. Por lo tanto, el contrato también debe describir los requisitos para disponer de los datos de forma adecuada cuando la organización a si lo considere. Si la propiedad de datos no se puede establecer correctamente, la organización puede optar por mover aquellos datos no sensibles y no críticos.	***Pregunta*** 22: ¿SLA?
No	Si la organización puede definir claramente la propiedad de los datos durante las negociaciones del contrato, los siguientes pasos para mover a la nube pueden ser abordados.	***Pregunta*** 20: ¿Jurisdicción?
20. ¿Jurisdicción?		
Si	A pesar de que la propiedad de los datos reside en la organización, las leyes locales e internacionales a menudo prohíben la transferencia o ciertos datos a los países que tienen leyes o reglamentos en conflicto. Por lo tanto, es importante para la organización conocer la ubicación de las instalaciones de almacenamiento de datos de la CSP y centros de procesamiento de datos para evitar infracciones legales. Es recomendable para la organización incluir en el contrato con el CSP las cláusulas necesarias que exijan al CSP limitar las ubicaciones de servicio a los aprobados por la organización.	***Pregunta*** 22: ¿SLA?
No	Si la organización no tiene limitación de la jurisdicción, la nube puede ser una solución adecuada.	***Solución***: Nube Privada
21. ¿Se puede actualizar?		

Si	Si se determina que la infraestructura actual de la organización no está preparado para integrarse con la nube, el siguiente paso es determinar si las necesidades del negocio son mayores que el costo de actualizar (análisis de viabilidad).	***Pregunta*** 17: ¿Predecible?
No	Si el costo para mejorar la infraestructura actual es mayor que las necesidades del negocio, la nube no puede ser una solución todavía.	***Solución***: La computación en nube puede no ser la mejor solución para sus necesidades de negocio actuales.
22. ¿SLA?		
Si	La organización debe determinar de antemano los términos que serán incluidos en el SLA, considerando que acuerdos estrictos o complejos podrían resultar en un mayor costo. Algunos de los términos que deben ser negociados y documentados en el SLA incluyen: • Disponibilidad • El tiempo de respuesta para las peticiones recursos de computación adicionales • Tiempo de respuesta de incidentes • Las políticas de copia de seguridad • Las políticas y procedimientos de retención y eliminación de datos • Gestión de Ruta • Los controles de seguridad • Recuperación y Continuidad objetivos • Controles para satisfacer los requisitos legales y de cumplimiento	***Pregunta*** 23: ¿Costo eficiente?
No	Si un SLA adecuada no puede ser acordado, trasladarse a la nube podría representar un nivel inaceptable de riesgo. Si el costo de la SLA es mayor que los beneficios del negocio, la solución de nube puede no ser la mejor solución.	***Solución***: La computación en nube puede no ser la mejor solución para sus necesidades de negocio actuales.
23. ¿Costo eficiente?		
Si	Dos de los principales objetivos de trasladarse a la nube constituye ser cada vez más rentable y ser capaz de reaccionar más rápida y económicamente a las situaciones cambiantes.	***Solución***: Nube Privada
No	A menos que los beneficios del negocio sea mayor que el costo, una solución cara puede no ser la opción correcta	***Solución***: La computación en nube puede no ser la mejor solución para sus necesidades de negocio actuales.

Tabla 2.2.3.3: Árbol de Decisión de Modelo de Despliegue en la Nube

En todo caso, las soluciones de nube hibrida se proyectan como la mejor opción futura, ya que son una alternativa viable para la mayoría de las organizaciones en la actualidad, pero la nube privada es el primer paso natural de ese camino, al brindar la mejor combinación de seguridad y rendimiento. La nube pública puede ser adecuada para aplicaciones seleccionadas en la actualidad, y más en el futuro a medida que la funcionalidad y la confiabilidad de las soluciones maduren.

2.2.3.2.4 Paso 4: Selección de Proveedor de la Nube

Toda vez que tanto a nivel directivo como operativo se ha establecido la factibilidad de incorporar la computación de nube ya sea para un activo de información piloto bajo un modelo de despliegue y modelo servicio previamente analizados, es necesario encontrar el Proveedor de Servicios de Nube (CSP) que mejor se adapte a las necesidades del negocio y que permita reducir al mínimo el riesgo potencial.

Si bien existen proveedores de nube pequeños que se adaptan a las necesidades de la organización, es importante elegir un proveedor de nube estable con referencias o caso de éxito comprobadas. Un proveedor estable o experimentado posiblemente posee mayor experticia con el funcionamiento de infraestructura de Nube, con la adaptación al cambio y por lo general con tiempos de respuesta mínimos frente a un incidente o amenaza, por tanto, son capaces de mantener la estabilidad de forma más eficiente, más aún dado la envergadura de la información que se maneja en la entidades del sector público ecuatoriano.

2.2.3.3 Fase III: Gestión De Riesgos

De acuerdo al marco de trabajo propuesto, esta fase del Modelo de Gestión de Riesgos de Infraestructura como Servicios (IaaS) de Cloud Computing aplicado a entidades del sector público ecuatoriano, se encuentra estructurado de acuerdo al esquema de la Figura 2.2.3.4, resultado de la identificación y acoplamiento de procesos y/o actividades de la norma ISO/IEC 27000, la metodología OCTAVE y el marco de trabajo COBIT con la Computación en la Nube.

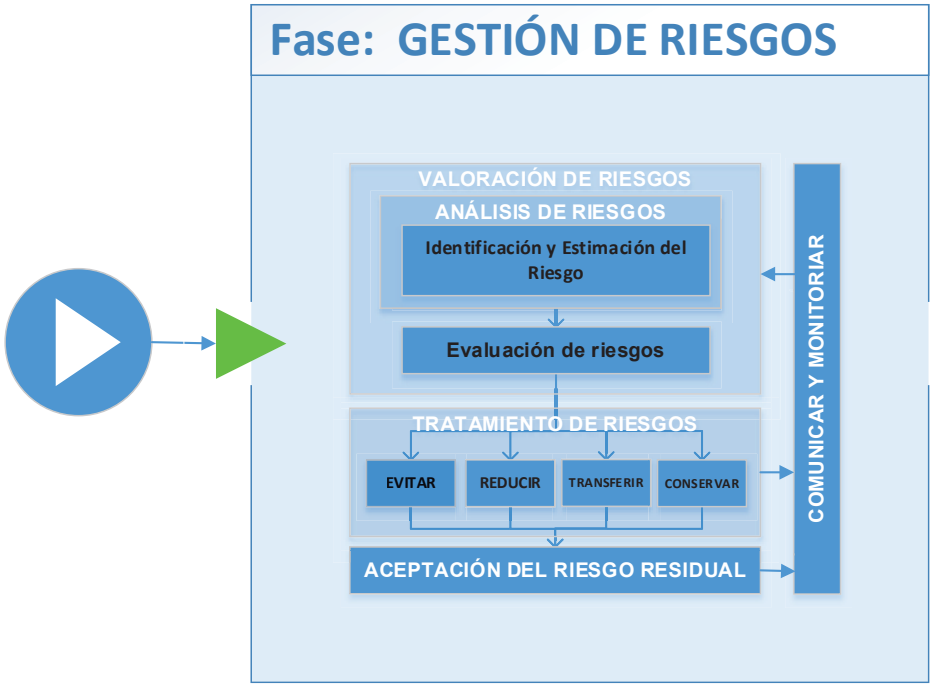

Figura 2.2.3.4 Gestión de Riesgos de Computación en la Nube

Esta fase permitirá a la entidad caso de estudio construir, ejecutar y supervisar una eficiente y efectiva función de gestión de riesgos para servicios en la Nube, alineado

a los objetivos estratégicos y a los niveles de tolerancia establecida por la alta dirección, que para este caso específico se encuentra representado por el Gobierno de Nube.

De acuerdo a la Figura 2.2.3.4, la Fase de gestión de Riesgos para servicios de Nube consta de la valoración del riesgos, el tratamiento del riesgos, la aceptación del riesgo y la comunicación, monitoreo y revisión del riesgo. Cada una con un enfoque iterativo que permite incrementar la profundidad y el detalle, reducir el tiempo y esfuerzo para cada etapa, garantizando una correcta gestión de riesgos. Es decir, si luego de realizar una valoración del riesgo, esta suministra información suficiente para determina de manera eficaz las acciones que se necesitan para modificar los riesgos hasta un nivel aceptable, entonces la labor está terminada y sigue la siguiente etapa de tratamiento del riesgo, caso contrario se realiza otra iteración de la valoración del riesgo, conforme lo planteado por el comité de gestión de riesgos. Proceso iterativo semejante para el resto de etapas de la Gestión de riegos.

Cabe indicar que a diferencia del modelo de gestión de riesgos de la ISO27000, no consta la etapa de “Establecimiento de Contexto”, ya que esta corresponde o forma parte de la “Fase II: Consideraciones Hacia la Nube” del modelo propuesto.

A continuación se describe brevemente los procesos y actividades esquematizados en la Figura 2.2.3.4:

2.2.3.3.1 Valoración del Riesgos

- ***Analizar los riesgos.-*** El análisis de riesgos implica la identificación de riesgos a partir de fuentes internas y externas, cada riesgo es evaluado para determinar su probabilidad y sus consecuencias. Estos riesgos se categorizan con base a la evaluación establecida en la estrategia de gestión de riesgos, proporcionando información suficiente para su manejo, estableciendo un nivel de análisis con base a lo que es apropiado y razonable. Para lo cual es necesario partir de la identificación de los activos más importantes de acuerdo al alcance, se identificará las áreas de interés, requisitos de seguridad y controles existentes para cada activo. Luego, se identificará las amenazas a partir de las áreas de interés, tomando como ayuda los perfiles de amenaza genéricos, catálogo de amenazas y vulnerabilidades. Finalmente, en este proceso se realizará la identificación de vulnerabilidades

tecnológicas a partir de la evaluación de los componentes de infraestructura seleccionados para el efecto.

- ***Evaluar los riesgos.-*** Este es el proceso donde se consolida la identificación, el análisis y la evaluación de los riesgos, es en este punto donde se determina la prioridad para el tratamiento adecuado. En esta etapa se realiza la identificación del impacto (consecuencia de un evento) a través de narraciones descriptivas para cada uno de los riesgos detectados en el proceso anterior, para la valoración del impacto será necesario comparar estas narraciones descriptivas con el criterio básico de impacto definido en el proceso de definición del contexto organizacional. De igual forma, para la valoración de la probabilidad, será necesario definir las descripciones de probabilidad para compararlas con el criterio de probabilidad que se define para este mismo proceso y es particular para cada riesgo y de la probabilidad del incidente. Posteriormente se debe aplicar la metodología de estimación del riesgo.

2.2.3.3.2 Tratar los Riesgos, Definir e Implementar los Planes de Mitigación.-

Terminada la evaluación del riesgo, se ejecutan las medidas correctivas donde se escogen una serie de opciones para mitigar el riesgo, este es un proceso repetitivo con el fin de determinar su tolerabilidad en contra de los criterios establecidos con el fin de decidir si se requiere un tratamiento posterior. Los riesgos son monitoreados cuando superen los umbrales establecidos, los planes de mitigación de riesgos se despliegan para devolver el esfuerzo afectado a un nivel de riesgo aceptable. Si el riesgo no puede ser mitigado, un plan de contingencia puede ser invocado.

El proceso de tratamiento al riesgo se ejecuta si es que la evaluación de riegos ha generado la suficiente información para determinar el tratamiento al riesgo, caso contrario será necesaria otra iteración sobre la definición del contexto organizacional.

De ser el caso, se define los lineamientos globales de protección a través de una estrategia de protección, posteriormente se establecerá los planes de mitigación en base al enfoque de riesgo (aceptar/mitigar). En caso de no llegar a un nivel de riesgo aceptable, en base a la comparación de los resultados del tratamiento con el criterio de aceptación del riesgo generado en el proceso de definición del contexto organizacional, será necesaria otra iteración a la evaluación de riesgo. Caso contrario, se determinará la lista de acciones a corto plazo y sin mayor requerimiento de entrenamiento, que pueden aplicarse para tratar

el riesgo. A partir de esto, se preparará una presentación para la alta directiva al respecto de los puntos clave de los riesgos y las soluciones propuestas. Finalmente se generará los siguientes pasos, es decir, información importante para aterrizar, apalancar e implementar la estrategia, plan y acciones.

2.2.3.3.3 Aceptar el Riesgo.-

En este punto del proceso, toma parte la alta dirección de la organización que es la encargada de determinar el nivel de impacto del riesgo y decidir si se acepta o no, teniendo en cuenta sus consecuencias. El aceptar el riesgo incluye en asumir las responsabilidades frente a las insuficiencias encontradas después de haber tratado el riesgo y ha quedado algún riesgo residual.

2.2.3.3.4 Llevar un Control de Seguimiento y Monitoreo del Riesgo Tratado.-

Como parte del proceso de gestión de riesgos, los riesgos y los controles deben ser monitoreados y revisados periódicamente para verificar que las hipótesis sobre los riesgos sigan siendo válidas, los supuestos en que se basa la evaluación del riesgo, incluyendo el contexto externa e interna sigan siendo válidos.
El proceso de comunicación del riesgo, se enfoca en que el riesgo debe ser continuamente comunicado y entendido entre los entes de decisión y los interesados, a través de la organización para la gestión de riesgos de seguridad de la información.

El proceso de monitoreo y revisión de riesgos se encarga de monitorear tanto los factores de riesgo así como la gestión de los riesgos, esto debido a que el riesgo y sus factores no son estáticos, permitiendo de esta forma mantener una imagen general del riesgo a través del tiempo, asegurando que los planes son los adecuados de acuerdo al contexto y que existen los recursos necesarios para llevarlos a cabo.

Dependiendo de la solución en la nube seleccionada, la organización podría utilizar múltiples proveedores y por tanto necesitara monitorear el desempeño de todas sus soluciones, siendo necesario que los proveedores proporcionen formatos consistentes para monitorizar el desempeño de los servicios haciéndolos compatibles con los sistemas de monitoreo existentes en la organización.

2.3 DETERMINACIÓN DE INDICADORES PARA LA GESTIÓN DE RIESGOS DE SERVICIOS DE CLOUD COMPUTING

Una vez que en el numeral 2.2 se estableciese la estrategia de integración de normas, metodologías y marcos de trabajo para la gestión de riesgos de servicio de Cloud Computing, se evidencia la necesidad de determinar controles apropiados para asegurar que los potenciales riesgos de Nube sean mitigados o reducidos a un nivel aceptable para la organización [7]. Actividades no contempladas en el temario original del plan de tesis, pero que de acuerdo al "Modelo de Gestión para un Proveedor de Cloud Computing [44]" la determinación de indicadores no son determinantes y útiles para un modelo de gestión de riesgos, ya que no se busca medir el nivel de éxito de un determinado proveedor de Nube, sino proponer medidas de mitigación a los potenciales riegos. Bajo ésta consideración, la presente sección se enfoca en la determinación de controles conforme lo planteado por la norma ISO 27000 – ver Figura 2.2.3.1 –, el marco de trabajo COBIT5 y las iniciativas de los líderes del mercado de Nube como lo son la CSA, el NIST y la ENISA.

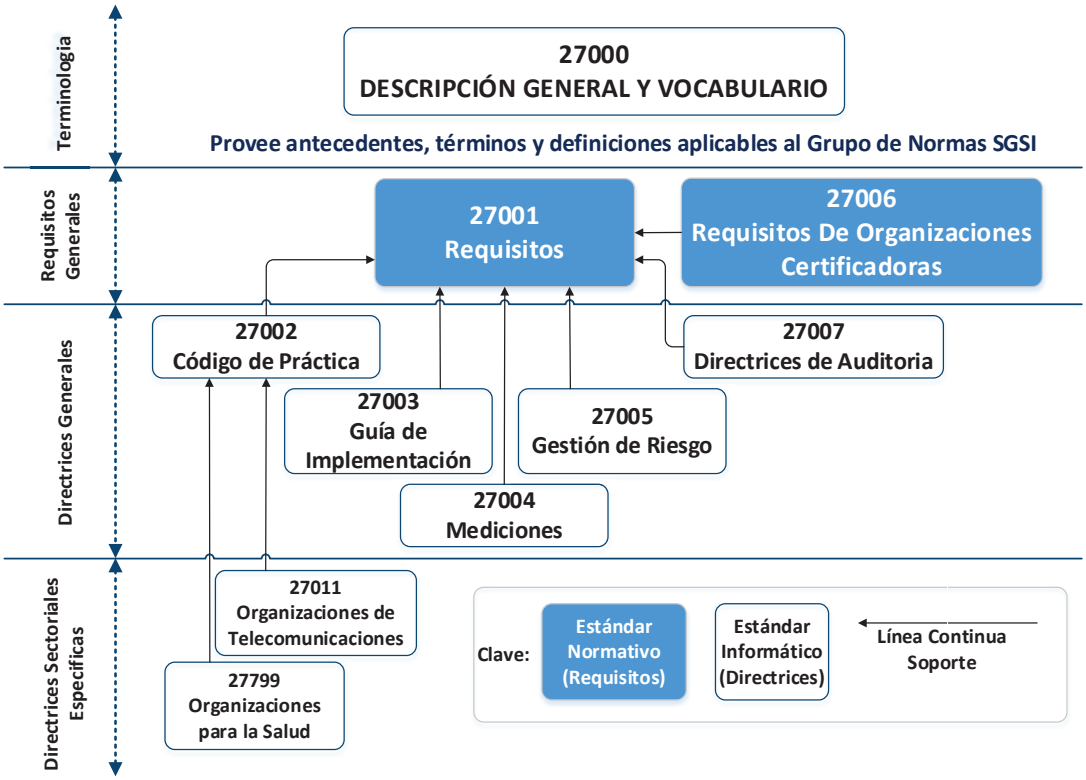

Figura 2.2.3.1 Relación del grupo de normas de SGSI [45].

Considerando que la norma ISO/IEC 27001 [45], entre otras cosas provee un grupo de controles para el manejo y mitigación de los riesgos, denominado Objetivos de Control y Controles del Anexo A, mismos que no son vinculantes y pueden ser adaptados a otros grupos de controles ya existentes (COBIT) o nuevos (Cloud Security Alliance), pero que se acoplen a las necesidades específicas de la organización, en esta sección se procederá a determinar controles para la gestión de riesgos de servicios de Cloud Computing, basados en iniciativas de los líderes del mercado, pero que guarden relación a las nomas o marcos de trabajo abordados en el numeral 2.1.

Una de las iniciativas más completa y de referencia internacional es la "Cloud Controls Matrix – CCM" [46] – cuya versión original y completa se encuentra publicado en el sitio web oficial de la Cloud Security Alliance Global, misma recoge los controles de referencia más importantes en seguridad en la Nube, para que proveedores y clientes dispongan de una guía completa para una adecuada adopción de servicios de Nube.

Para el caso específico del presente trabajo, la CCM ha sido adaptada para que cubra tanto aspectos de cumplimiento y gobierno, como de arquitectura y de tipo técnico contemplado en el Modelo de Gestión de Riesgos de Infraestructura como Servicios (IaaS) de Cloud Computing aplicado a entidades del sector público ecuatoriano, lo que permitirá reducir los riesgos, las amenazas y las vulnerabilidades en la nube. Como resultado se ha logrado identificar 33 controles, mismos que guardan relación con el marco de trabajo COBIT5 y la ISO27001, como se puede apreciar en la Tabla 2.3.1.

CONTROL	DESCRIPCIÓN	USUARIO/CLIENTE	GUBERNAMENTAL	TIPO DESPLIEGUE IaaS	ARQUITECTURA FÍSICA	COBIT5	ISO/IEC27001
Seguridad de Aplicaciones e Interfaces. Requerimientos de acceso de clientes	Antes de conceder a los clientes el acceso a los datos, activos y sistemas de información, todos los requisitos identificados de seguridad, contractuales y reglamentarios sobre el acceso de los clientes deberán ser considerados y corregidos.	X	X	X	X	APO09.01 APO09.02 APO09.03 APO13.01 BAI02 DSS05	A.6.2.1 A.6.2.2 A.11.1.1

Cumplimiento y aseguramiento de las Auditorías. Auditorías Independientes	Las revisiones independientes y las evaluaciones se llevarán a cabo al menos anualmente, o en intervalos planificados, para asegurarse de que la organización resuelve cualquier no conformidad de las políticas establecidas, los procedimientos y el cumplimiento de las obligaciones contractuales, estatutarias o reguladoras.	X	X	X	X	APO12.04 APO12.05 DSS05.07 MEA02.06 MEA02.07 MEA02.08 MEA03.01	4.2.3e 5.1 g 5.2.1 d) 6 A.6.1.8
Cumplimiento y aseguramiento de las Auditorías. Mapa de regulación de los sistemas de información	Se deberá mantener un inventario de las obligaciones externas legales, estatutarias y reglamentarias de la organización asociado (y mapeado) con cualquier alcance y presencia geográfica, y que considere datos relevantes o información propiedad de la organización y administrada por la infraestructura de red (física o virtual) y los componentes de los sistemas, actualizado periódicamente según las necesidades del negocio (por ejemplo, un cambio en el alcance y/o un cambio en las obligaciones).	X	X	X	X	APO12.01 APO12.02 APO12.03 MEA03.01	4.2.1 b) 2) 4.2.1 c) 1) 4.2.1 g) 4.2.3 d) 6) 4.3.3 5.2.1 a - f 7.3 c) 4) A.7.2.1 A.15.1.1 A.15.1.3 A.15.1.4 A.15.1.6
Gestión de la Continuidad del Negocio y Resiliencia Operacional. Planificación de la Continuidad de Negocio	Debe establecerse un marco unificado y consistente para la planificación de la continuidad de negocio y debe desarrollarse un plan, documentado y adaptado, para asegurar que todos los planes de continuidad del negocio son consistentes en el tratamiento de las prioridades, las pruebas, el mantenimiento y los requisitos de seguridad de la información. Los requisitos para los planes de continuidad del negocio deben incluir los siguientes: • Un propósito y alcance definidos y en línea con las dependencias pertinentes • Accesible y comprensible para los que van a utilizarlos • Identificación de una(s) persona(s) nombrada(s) que es(son) responsable(s) de su revisión, actualización y aprobación • Las líneas de comunicación específicas, los roles y las responsabilidades deberán estar definidos • Los procedimientos de recuperación, los manuales de trabajo y la información de referencia están detallados. • Hay un método para la invocación del plan	X	X	X	X	DSS04.01 DSS04.02 DSS04.03 DSS04.05	5.1 A.6.1.2 A.14.1.3 A.14.1.4
Gestión de la Continuidad del Negocio y Resiliencia Operacional. Pruebas de Continuidad de Negocio	Los planes de respuesta ante incidentes de seguridad y de continuidad de negocio estarán sometidos a pruebas en los intervalos planificados o cuando se produzcan cambios organizativos o ambientales significativos. Los planes de respuesta ante incidentes deberán implicar a los clientes (arrendatarios) afectados y a otras relaciones comerciales que representen dependencias críticas de procesos de negocio dentro de la cadena de suministro.	X	X	X	X	DSS04.04	A.14.1.5
Gestión de la Continuidad del Negocio y Resiliencia Operacional.	Deberá existir un procedimiento definido y documentado para determinar el impacto de cualquier interrupción en la organización, que deberá incorporar los siguientes aspectos:	X	X	X	X	BAI06.01 BAI10.01 BAI10.02 BAI10.03 DSS04.01 DSS04.02	A.14.1.2 A 14.1.4

Análisis de Impacto	• Identificar los productos y servicios críticos • Identificar todas las dependencias, incluyendo procesos, aplicaciones, socios comerciales y proveedores de servicios externos • Comprender las amenazas a los productos y servicios críticos • Determinar los impactos resultantes de interrupciones planificadas o no planificadas y cómo éstos varían con el tiempo • Establecer el período máximo tolerable de interrupción • Establecer prioridades para la recuperación • Establecer los objetivos de tiempo de recuperación para la reanudación de los productos y servicios críticos dentro de su período máximo tolerable de interrupción • Estimar los recursos necesarios para la reanudación						
Gestión de la Continuidad del Negocio y Resiliencia Operacional. Programa de Gestión	Se establecerán las políticas y los procedimientos y se implementarán las medidas técnicas de apoyo a los procesos de negocio para la resiliencia, la continuidad operativa y la gestión de los riesgos relacionados con las interrupciones de negocio, ya sean menores o catastróficas. Estas políticas, procedimientos, procesos y medidas deben proteger la disponibilidad de las operaciones críticas del negocio y los activos de la organización, de conformidad con las obligaciones de cumplimiento legal, estatutaria o reglamentarias aplicables. Se implementará un programa de gestión con las funciones y responsabilidades de soporte, que haya sido comunicado, y en caso necesario, contractualmente convenido por todas las instalaciones afectadas, el personal y/o las relaciones comerciales externas.	X	X	X	X		4.3.2 A.14.1.1 A 14.1.4
Seguridad del Centro de Datos. Equipamiento fuera de las instalaciones	Se deberá establecer políticas y procedimientos apoyando los procesos de negocio implementados para el uso y eliminación segura del mantenimiento de equipos y el uso fuera de las instalaciones de la organización.	X	X	X	X	APO09.03 APO10.04 APO10.05 APO13.01 DSS01.02	A.7.1.1 A.7.1.2
Gobierno y Gestión del Riesgo. Programa de Gestión	Un programa de gestión en seguridad de la información debe estar desarrollado, documentado, aprobado, e implementado, incluyendo medidas administrativas, técnicas y físicas para proteger activos y datos de la pérdida, el acceso no autorizado, el uso indebido, la divulgación, la alteración y la destrucción. El programa de seguridad debe incluir, pero no debe estar limitado, por las siguientes áreas, desde el momento en que éstas están relacionadas con las características del negocio: • Gestión de riesgos • Política de seguridad • Organización de la seguridad de la información • Gestión de activos • Seguridad de recursos humanos • Seguridad física y del entorno	X	X	X	X	APO13.01 APO13.02 APO13.03	4.2 5 A.6.1.1 A.6.1.2 A.6.1.3 A.6.1.4 A.6.1.5 A.6.1.6 A.6.1.7 A.6.1.8

	• Gestión de comunicaciones y operaciones • Control de acceso • Adquisición de sistemas de información, desarrollo y mantenimiento.						
Gobierno y Gestión del Riesgo. Impacto de la Política en las Evaluaciones del Riesgo	Los resultados de la evaluación de riesgos deberán incluir actualizaciones de las políticas de seguridad, de los procedimientos, de las normas y los controles, para asegurar que estos documentos permanecen relevantes y efectivos.	X	X	X	X	APO12 APO13.01 APO13.03	4.2.3 4.2.4 4.3.1 5 7 A.5.1.2 A.10.1.2 A.10.2.3 A.14.1.2 A.15.2.1 A.15.2.2
Gobierno y Gestión del Riesgo. Análisis de Riesgo	Un análisis de riesgos formalizado, alineado con los objetivos de la organización, deberá ser realizado al menos una vez al año o a intervalos planificados para determinar la probabilidad e impacto de todos los riesgos identificados, usando métodos cuantitativos o cualitativos. La probabilidad y el impacto asociado con el riesgo intrínseco y residual deberá estar determinado independientemente, considerando todas las categorías de riesgo (por ejemplo, con el resultado de las auditorías, el análisis de vulnerabilidades y amenazas y el cumplimiento normativo).	X	X	X	X	APO12	4.2.1 c) – g) 4.2.3 d) 5.1 f) 7.2 & 7.3 A.6.2.1 A.12.5.2 A.12.6.1 A.14.1.2 A.15.1.1 A.15.2.1 A.15.2.2
Gobierno y Gestión del Riesgo. Sistema de Gestión del Riesgo	Las organizaciones desarrollarán y mantendrán un sistema de gestión de riesgos para mitigar el riesgo a un nivel aceptable.	X	X	X	X	EDM03.02 APO01.03 APO12	4.2.1 c) – g) 4.2.2 b) 5.1 f) 7.2 & 7.3 A.6.2.1 A.12.6.1 A.14.1.2 A.15.2.1 A.15.2.2
Gobierno y Gestión del Riesgo. Mitigación / Aceptación del Riesgo	Los riesgos deben mitigarse a un nivel aceptable. Los niveles de aceptación basados en criterios de riesgo deben establecerse y documentarse conforme a un tiempo de resolución razonable y una aprobación ejecutiva	X	X	X	X		4.2.1 c) – g) 4.2.2 b) 4.3.1 5.1 f) 7.3 A.6.2.1 A.12.5.2 A.12.6.1 A.15.1.1 A.15.2.1 A.15.2.2
Recursos Humanos. Devolución de Activos	A la finalización del contrato de trabajo y/o la finalización de las relaciones comerciales externas, los activos propiedad de la organización deben ser devueltos dentro del periodo establecido.	X	X	X	X	APO01.08 APO07.06 APO13.01 BAI09.03	A.7.1.1 A.7.1.2 A.8.3.2
Recursos Humanos. Contratos laborales	Los contratos laborales deberán incorporar las cláusulas y/o los términos de cumplimiento para establecer el gobierno de la información y las políticas de seguridad y deberán ser firmados en las nuevas contrataciones o por el nuevo personal (por ejemplo, empleados a tiempo total o parcial o trabajadores eventuales), y siempre con anterioridad a proporcionar el acceso al usuario a los servicios de la organización, recursos y activos.	X	X	X	X	APO01.03 APO13.01 APO07.06 APO09.03 APO10.01	A.6.1.5 A.8.1.3

Recursos Humanos. Gestión de dispositivos móviles	Se establecerán las políticas y los procedimientos y se implementarán las medidas técnicas de apoyo para gestionar el riesgo de negocio asociado a que esté permitido que los dispositivos móviles accedan a recursos corporativos, pudiendo requerir de la implementación o controles compensatorios de seguridad más altos para su uso aceptable (por ejemplo, formación por mandato de seguridad, autenticación fuerte, derechos y controles de acceso y monitorización de dispositivos).	X	X	X	X	APO01.08 APO13.01 APO13.02 DSS05.01 DSS05.02 DSS05.03 DSS05.07 DSS06.03 DSS06.06	A.7.2.1 A.10.7.1 A.10.7.2 A.10.8.3 A.11.7.1 A.11.7.2 A.15.1.4
Recursos Humanos. Roles / Responsabilidades	Los roles y responsabilidades de contratistas, empleados y terceras partes deberán estar documentadas en lo que respecta a los activos de información y seguridad.	X	X	X	X	APO01.02 APO01.03 APO01.08 APO07.06 APO09.03 APO10.04 APO13.01 APO13.03	5.1 c) A.6.1.2 A.6.1.3 A.8.1.1
Recursos Humanos. Formación / Concienciación	Un programa de concienciación debe establecerse para todos los proveedores, usuarios de terceras-partes y empleados de la organización y exigido cuando sea conveniente. Todas las personas con acceso a datos de la organización recibirán una formación de forma regular en procedimientos de la organización, procesos y políticas relacionada con su función profesional respecto a la organización.	X	X	X	X	APO01.03 APO01.08 APO07.03 APO07.06 APO13.01 APO13.03	5.2.2 A.8.2.2
Recursos Humanos. Responsabilidad de los Usuarios	Se deberá hacer consciente a todo el personal de sus roles y responsabilidades para: • Mantener el cumplimiento y concienciación respecto a las políticas y procedimientos establecidos así como con la legislación aplicable y obligaciones de cumplimiento regulatorio. • Mantener un entorno de trabajo seguro.	X	X	X	X	APO01.02 APO01.03 APO01.08 APO07.03 APO07.06 APO13.01 APO13.03	5.2.2 A.8.2.2 A.11.3.1 A.11.3.2
Recursos Humanos. Lugares de trabajo	Las políticas y procedimientos establecerán requerimientos para que en los lugares de trabajo sin personal presente no existan (por ejemplo, sobre la mesa) documentos de contenido sensible totalmente accesibles y las sesiones de usuario iniciadas en el equipo informático hayan sido bloqueadas tras un período determinado de inactividad.	X	X	X	X	APO01.02 APO01.03 APO01.08 APO07.03 APO07.06 APO13.01 APO13.03 DSS05.03 DSS06.06	5.2.2 A.8.2.2 A.9.1.5 A.11.3.1 A.11.3.2 A.11.3.3
Gestión de Identidades y Accesos. Acceso por Terceros	La identificación, evaluación y priorización de los riesgos planteados por los procesos de negocio que requieren acceso de terceros a los datos y sistemas de información de la organización deberán ir seguidos de la aplicación coordinada de recursos para minimizar, monitorizar y medir la probabilidad y el impacto de accesos no autorizados o inapropiados. Los controles compensatorios derivados del análisis de riesgos se implantarán antes de la provisión de acceso.	X	X	X	X	APO01.03 APO01.08 APO07.06 APO10.04 APO13.02 DSS05.04 DSS05.07 DSS06.03 DSS06.06	A.6.2.1 A.8.3.3 A.11.1.1 A.11.2.1 A.11.2.4
Seguridad de la Infraestructura y Virtualización. Seguridad Inalámbrica	Se establecerán políticas y procedimientos, así como apoyo a los procesos de negocio y las medidas técnicas implementadas, para proteger los entornos de red inalámbrica, incluyendo las siguientes:	X	X	X	X	APO01.08 APO13.01 APO13.02 DSS02.02 DSS05.02 DSS05.03	A.7.1.1 A.7.1.2 A.7.1.3 A.9.2.1 A.9.2.4 A.10.6.1

	• Firewalls perimetrales implementados y configurados para restringir el tráfico no autorizado • Configuraciones de seguridad habilitadas con cifrado robusto para la autenticación y transmisión reemplazando la configuración por defecto del fabricante (por ejemplo, claves de cifrado, contraseñas y SNMP "community strings") • Acceso de usuario a dispositivos de red inalámbricos restringido a personal autorizado • Capacidad de detectar la presencia de dispositivos de red inalámbricos no autorizados (rogue) para una desconexión oportuna de la red					DSS05.04 DSS05.05 DSS05.07 DSS06.03 DSS06.06	A.10.6.2 A.10.8.1 A.10.8.3 A.10.8.5 A.10.10.2 A.11.2.1 A.11.4.3 A.11.4.5 A.11.4.6 A.11.4.7 A.12.3.1 A.12.3.2
Gestión de incidentes de seguridad, Localización de evidencias electrónicas, Investigaciones forenses en la nube Puntos de contacto con las autoridades	Se deberán mantener disponibles y actualizados los puntos de contacto de las fuerzas de seguridad locales y nacionales, autoridades legislativas aplicables y otras autoridades con jurisdicción legal (sobre todo en caso de cambios en el alcance o en las obligaciones de cumplimiento), de modo que se asegure el establecimiento directo de los enlaces correspondientes y la disposición para una investigación forense que requiera una participación rápida de las fuerzas de seguridad.	X	X	X	X	APO01.01 APO01.02 APO01.03 APO01.08 MEA03.01 MEA03.02 MEA03.03	A.6.1.6 A.6.1.7
Gestión de incidentes de seguridad, Localización de evidencias electrónicas, Investigaciones forenses en la nube Gestión de incidentes	Se deberán establecer procedimientos y políticas, así como medidas técnicas y procesos de negocio de apoyo, que permitan la evaluación y clasificación de eventos de seguridad y que garanticen una gestión completa y en tiempo de los incidentes así como sea establecido en las políticas y procedimientos de gestión de servicios TI.	X	X	X	X	APO01.03 APO13.01 APO13.02 DSS01.03 DSS02.01 DSS02.02 DSS02.04 DSS02.05 DSS02.06	4.3.3 A.13.1.1 A.13.2.1
Gestión de incidentes de seguridad, Localización de evidencias electrónicas, investigaciones forenses en la nube Comunicación de incidentes	Se deberá informar a los trabajadores y a las organizaciones externas relacionadas acerca de sus responsabilidades y, si fuera necesario, deberán dar su consentimiento o aceptar contractualmente a informar prontamente de todos los eventos de seguridad. Los eventos de seguridad deberán ser comunicados a través de canales de comunicación predefinidos oportunamente cumpliendo con las obligaciones legales, reglamentarias o de cumplimiento regulatorio aplicables.	X	X	X	X	APO01.03 APO07.06 APO07.03 APO13.01 APO13.02 DSS02.01	4.3.3 5.2.2 A.6.1.3 A.8.2.1 A.8.2.2 A.13.1.1 A.13.1.2 A.13.2.1
Gestión de incidentes de seguridad, Localización de evidencias electrónicas, investigaciones forenses en la nube Preparaciones legales para la respuesta ante incidentes	En el caso de que una investigación posterior que afecte a una persona u organización después de un incidente de seguridad requiera acciones legales se exige el seguimiento de los debidos procedimientos forenses, incluyendo la cadena de custodia, para la preservación y presentación de las pruebas que apoyen dichas acciones legales ante la jurisdicción pertinente. Tras la notificación, los clientes (arrendatarios) y/o las relaciones con otras organizaciones externas que hayan sido afectadas por una violación de seguridad deberán tener la oportunidad de participar como sea legalmente posible en la investigación forense.	X	X	X	X	APO01.03 APO13.01 APO13.02 DSS01.03 DSS02.01 DSS02.02 DSS02.04 DSS02.05 DSS02.06	4.3.3 5.2.2 A.8.2.2 A.8.2.3 A.13.2.3 A.15.1.3

Gestión de incidentes de seguridad, Localización de evidencias electrónicas, investigaciones forenses en la nube Métricas de la respuesta ante incidentes	Se deberán implantar los mecanismos que permitan monitorizar y cuantificar los tipos, cantidades y costes de los incidentes de seguridad de la información.	X	X	X	X	DSS04.07	A.13.2.2
Gestión de la cadena de suministro, Transparencia y Responsabilidad Servicios de red / infraestructura	Los componentes de la infraestructura de sistemas y redes, así como el diseño y configuración de las aplicaciones (físicas y virtuales) y de los interfaces sistema-sistema (API) que sean críticos para el negocio o que impacten al cliente (arrendatario) deberán ser diseñados, desarrollados y desplegados de acuerdo con unas expectativas de nivel de servicio y capacidad acordadas previamente, así como de acuerdo a las políticas y procedimientos de gestión de servicio y gobernanza TI.	X	X	X	X	APO01.03 APO03.01 APO03.02 APO09.03 BAI02.01 BAI02.04 BAI07.05	A.6.2.3 A.10.6.2
Gestión de la cadena de suministro, Transparencia y Responsabilidad Acuerdos relativos a la cadena de suministro	Los Acuerdos de la cadena de suministro (por ejemplo, SLA) entre proveedores y clientes (arrendatarios) contendrán al menos las siguientes mutuamente acordadas disposiciones y/o los términos: • Alcance de la relación comercial y de servicios que se ofrece (por ejemplo , adquisición de datos del cliente (arrendatario), el intercambio y el uso, conjuntos de características y funcionalidad , el personal y la infraestructura de red y componentes de los sistemas de prestación de servicios y apoyo, roles y responsabilidades de proveedor y cliente (arrendatario) y cualquier relación comercial subcontratada o externalizada, la ubicación geográfica física de los servicios de hospedaje , y cualquier aspecto de cumplimiento regulatorio conocidos) • Los requisitos de seguridad de la información, los puntos de contacto principales durante la duración de la relación comercial del proveedor y el cliente (arrendatario), y las referencias a la información detallada de apoyo y procesos de negocio relevantes y medidas técnicas implementadas para permitir el gobierno efectivo, la gestión de riesgos y cumplimiento de las obligaciones de seguridad, legales, estatutaria y normativas por todas las partes afectadas. • Notificación y/o pre- autorización los cambios controlados por el proveedor con impacto en el cliente (arrendatario) • La notificación a tiempo de un incidente de seguridad (o brecha de seguridad confirmada) a todos los clientes (arrendatarios) y otras partes afectadas (es decir, hacia arriba y debajo de la cadena de suministro afectada) • Evaluación y verificación independiente del cumplimiento de las	X	X	X	X		A.6.2.3 A10.2.1 A.10.8.2 A.11.4.6 A.11.6.1 A.12.3.1 A.12.5.4

	disposiciones del acuerdo y / o términos (por ejemplo, la certificación aceptable para la industria, el informe de auditoría de certificación, o formas equivalentes de aseguramiento) sin representar un riesgo de negocio inaceptable de la exposición para la organización que está siendo evaluada • Finalización de la relación comercial y el tratamiento de los datos del cliente (arrendatario) afectados • El cliente (arrendatario) de una aplicación servicio a servicio (API) y los requerimientos de interoperabilidad y portabilidad de los datos para el desarrollo de aplicaciones y el intercambio de información, el uso y la persistencia de la integridad						

Tabla 2.3.1: Controles para servicios de Cloud Computing

En la Tabla 2.3.1, no se consideran la metodología OCTAVE, por cuanto es una técnica efectiva que establece el cómo implementar las guías de gestión de riesgos de la ISO/IEC 27005.

CAPITULO 3

VALIDACIÓN DEL MODELO EN UN CASO DE ESTUDIO.

La validación del Modelo de Gestión de Riesgos de Infraestructura como Servicios (IaaS) de Cloud Computing propuesto, se lo realizará mediante la aplicación de sus fases al "Sistema Integrado de Recaudación del Transporte Público Urbano de los cantones de Santa Elena, la Libertad y Salinas" que posee la Agencia Nacional de Transito, cuyos resultados serán puestos a consideración del Directorio, quién determinará su efectividad mediante la aplicación al resto de sistemas o activos de información que estén pretendiendo ser migrados hacia la Nube.

En adelante al "Sistema Integrado de Recaudación del Transporte Público Urbano de los cantones de Santa Elena, la Libertad y Salinas" se lo identificara como Sistema Recaudo.

3.1 ANÁLISIS SITUACIONAL DE LA ENTIDAD CASO DE ESTUDIO.

El análisis situacional de la entidad caso de estudio, tiene por objeto contribuir a un entendimiento sobre su actividad principal con la intensión de tener un marco de referencia que permita valorar la inclusión de la gestión de riesgos en proyectos institucionales y de gestión que se relacionen con la Computación en la Nube.

Considerando que, es obligación del Estado garantizar la libertad de transporte terrestre dentro del territorio nacional, sin privilegios de ninguna naturaleza y bajo los principios de seguridad, eficiencia, responsabilidad, universalidad, accesibilidad, continuidad y calidad [47], mediante Registro Oficial Suplemento No. 415 de 29 de marzo del 2011 [48], el Pleno de la Asamblea Nacional Constituyente, expidió la Ley Orgánica Reformatoria a la Ley Orgánica de Transporte Terrestre, Tránsito y Seguridad Vial – LOTTTSV, con la que se creó la Agencia Nacional de Regulación y Control del Transporte Terrestre, Tránsito y Seguridad Vial – en adelante Agencia Nacional de Tránsito A.N.T. – a fin de que subrogue los derechos,

obligaciones, patrimonio, bienes y personal de la antes Comisión Nacional de Transporte Terrestre, Tránsito y Seguridad Vial, que por efecto de las reformas cesó en su vida jurídica.

Preceptos generales de la normativa antes referida, que faculta a la Agencia Nacional de Tránsito a planificar, fomentar, regular, modernizar y controlar el Transporte Terrestre, Tránsito y Seguridad Vial en el territorio nacional, con sujeción a las políticas emanadas del Ministerio del Sector; con el fin de proteger a las personas y bienes que se trasladan de un lugar a otro por la red vial del territorio ecuatoriano, y a las personas y lugares expuestos a las contingencias de dicho desplazamiento, contribuyendo al desarrollo socio-económico del país en aras de lograr el bienestar general de los ciudadanos.

3.1.1 MISIÓN, VISIÓN, OBJETIVOS Y POLÍTICAS INSTITUCIONALES.

De conformidad al Estatuto Orgánico de Gestión Organizacional por Procesos de la Agencia Nacional de Tránsito, expedida por la Dirección Ejecutiva de la Agencia Nacional de Tránsito, mediante Registro Oficial Suplemento No. 323 [49], de 17 de agosto de 2012, se establece:

- ***Visión***: "Ser la entidad líder que regule y controle el ejercicio de las competencias de transporte terrestre, tránsito y seguridad vial, basados en la transparencia y calidad de servicio que garanticen a la sociedad ecuatoriana una regulación eficaz mediante la planificación y control del transporte terrestre, tránsito y seguridad vial".

- ***Misión***.- "Planificar, regular y controlar la gestión del Transporte Terrestre, Tránsito y Seguridad Vial en el territorio nacional, a fin de garantizar la libre y segura movilidad terrestre, prestando servicios de calidad que satisfagan la demanda ciudadana; coadyuvando a la preservación del medio ambiente y contribuyendo al desarrollo del País, en el ámbito de su competencia".

- ***Objetivos***.- "Contribuir al desarrollo nacional a través de regulación, planificación y control del transporte terrestre, tránsito y seguridad vial – TTTSV –, mediante la formulación y aplicación de leyes, normas, políticas, planes, programas y proyectos que garanticen la satisfacción de los usuarios".

- Desarrollar regulaciones que permitan una gestión óptima y un control eficiente del transporte terrestre, tránsito y seguridad vial, a fin de asegurar el libre tránsito y seguridad de personas y bienes en el país.
- Implementar el modelo de gestión institucional que permita el desarrollo de los procesos de desconcentración y descentralización de competencias asignadas por ley, a fin de modernizar la administración del sector del transporte terrestre y seguridad vial a nivel nacional.
- Implementar sistemas de planificación y control administrativo del tránsito, transporte terrestre y seguridad vial, a través de regulaciones sectoriales, planes, programas y proyectos ejecutados por las distintas direcciones de la institución que permitan cumplir la misión de la ANT.
- Impulsar el desarrollo del transporte terrestre, tránsito y seguridad vial, así como su mejoramiento continuo, mediante la suscripción y aplicación de convenios con entidades nacionales e internacionales.

- ***Políticas***: Entre las principales políticas que identifican a la Agencian Nacional de Transito se tiene:
  - Promover la implementación de indicadores de gestión operativa, administrativa y presupuestaria.
  - Generar mecanismos de control en materia de transporte terrestre en sus diversas modalidades.
  - Controlar técnicamente el cumplimiento de regulaciones, normativas técnicas y legales en la gestión del transporte terrestre, tránsito y seguridad vial, así como la prestación de los servicios de transporte terrestre en sus diversas modalidades.
  - Coordinar con los GAD´s, la ejecución de programas, planes y proyectos integrales.
  - Aplicar procesos y procedimientos institucionales de ejecución presupuestaria, en coordinación con los órganos reguladores y de control.
  - Coordinar con los gobiernos sectoriales y locales la ejecución de programas y acciones para la regulación y control de los servicios de transporte.

3.1.2 ESTRUCTURA ORGANIZACIONAL:

La Agencia Nacional de Tránsito, para el cumplimiento de su misión, objetivos y políticas, se encuentra integrada en el ámbito de su competencia por procesos Gobernantes, procesos Agregadores de Valor y procesos Habilitantes, esquematizados en el mapa de procesos de la Figura 3.1.2.1.

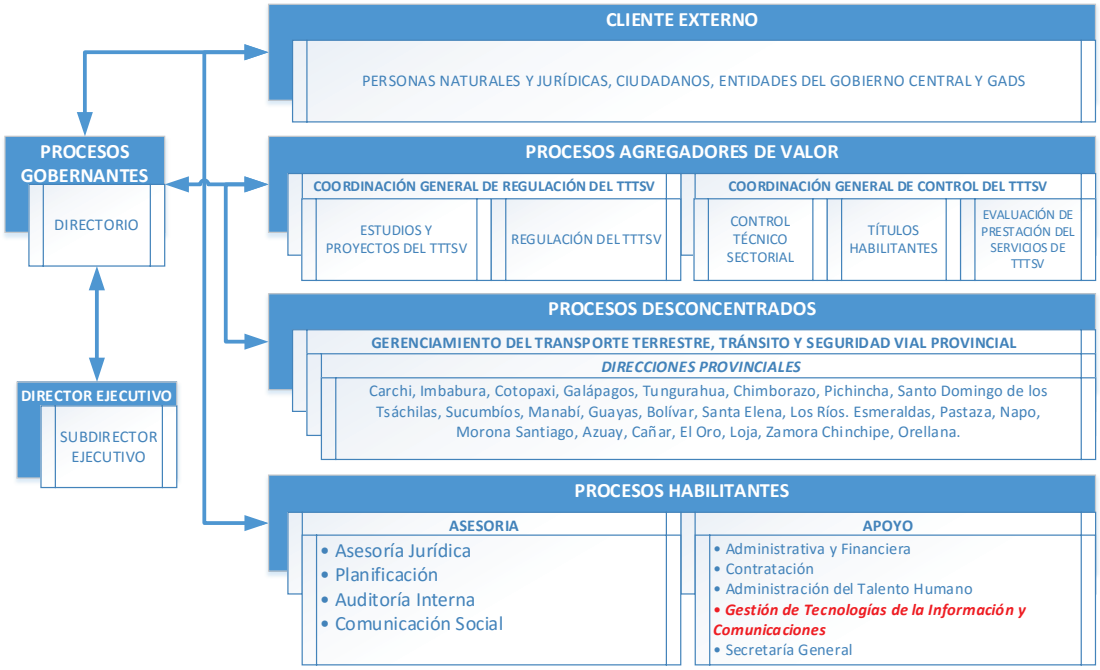

Figura 3.1.2.1 Mapa de procesos Agencia Nacional de Tránsito [49].

Cada grupo de Procesos de la Figura 3.1.2.1, representa una visión general de la estructura organizacional de la Agencia Nacional de Tránsito, con funciones y atribuciones específicas e integradas por unidades técnicas, jurídicas, administrativas y financieras interrelacionadas entre sí, que se sintetizan en el orgánico funcional esquematizado en la Figura 3.1.2.2:

- ***Procesos Gobernantes***.- Responsables de la formulación de la política institucional interna, lineamientos, planes estratégicos, generación de directrices y expedición de normas e instrumentos para el desempeño de la entidad, así como también del cumplimiento de la política emitida por el Órgano Rector del transporte nacional.

- ***Agregadores de Valor***.- Responsables de generar el portafolio de productos y servicios primarios requeridos por los clientes externos, en cumplimiento de la misión institucional; constituyen la razón de ser de la Organización.

- ***Habilitantes***.- Se clasifican en procesos de asesoría y procesos de apoyo. Están encaminados a generar productos y servicios secundarios en apoyo a la gestión de los procesos gobernantes, agregadores de valor y viabilizan la consecución de objetivos y metas institucionales.

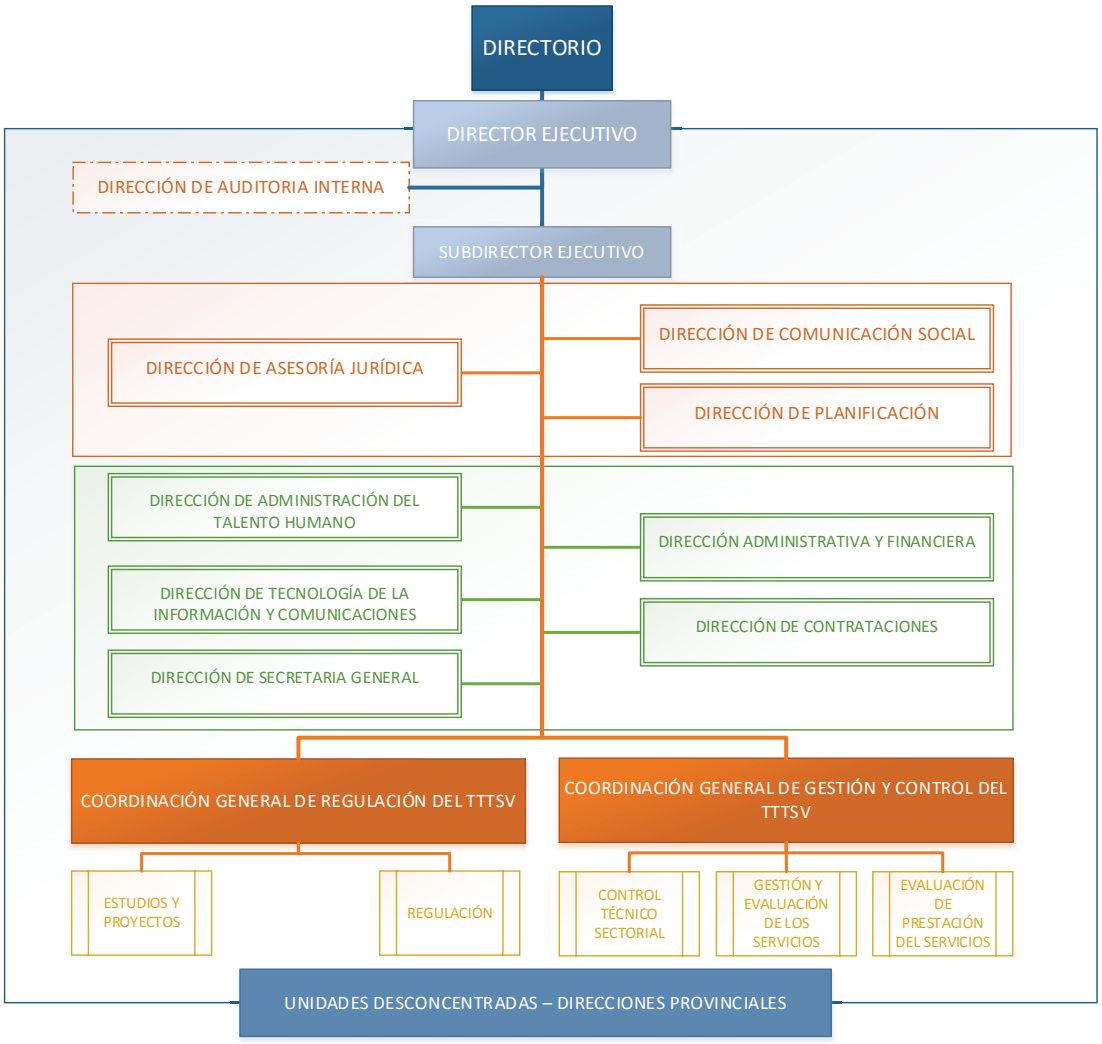

Figura 3.1.2.2 Estructura Orgánico Funcional Agencia Nacional de Tránsito [49].

Del orgánico funcional de la Figura 3.1.2.2, es necesario establecer las funciones, atribuciones y prohibiciones a las que se deben acoger el nivel directivo de la Agencia Nacional de Tránsito.

3.1.2.1 Directorio de la Agencia Nacional de Tránsito.

De conformidad a la Ley Orgánica Reformatoria a la LOTTTSV, la Agencia Nacional de Tránsito es una entidad autónoma de derecho público, con personería jurídica, jurisdicción nacional, presupuesto, patrimonio y régimen administrativo y financiero propio, con domicilio en el Distrito Metropolitano de Quito.

La Agencia Nacional de Tránsito es regida por un Directorio, que sesiona en forma ordinaria una vez al mes; y, extraordinariamente cuando lo convoca su Presidente o a solicitud de al menos tres de sus miembros. Sus resoluciones se adoptan por mayoría absoluta de votos, donde el Presidente tiene voto dirimente [48].

El directorio de la Agencia Nacional de Tránsito, se encuentra integrado de la siguiente forma:

- El Ministro del Sector o su delegado que será el Subsecretario responsable del Transporte Terrestre, Tránsito y Seguridad Vial, quien lo presidirá;
- El Ministro del Sector de la Salud o su delegado;
- El Ministro del Sector de la Educación o su delegado;
- Un representante designado por el Presidente de la República;
- Un representante por los Gobiernos Autónomos Descentralizados Regionales, Metropolitanos y Municipales que tengan más de un millón de habitantes; y,
- Un representante por los Gobiernos Autónomos Descentralizados Regionales, y Municipales

Entre las funciones y atribuciones del Directorio de la Agencia Nacional de Tránsito se tiene:

- Establecer, controlar y auditar las regulaciones en materia de transporte terrestre, tránsito y seguridad vial, por parte de los Gobiernos Autónomos Descentralizados – GAD´s;
- Supervisar y controlar a las operadoras nacionales e internacionales de transporte terrestre y demás instituciones prestadoras de servicios de tránsito y seguridad vial;
- Expedir los reglamentos necesarios para el cumplimiento de sus fines y objetivos; y,

- Nombrar al Director Ejecutivo de la Institución.

Siendo una de sus prohibiciones el de tomar parte, interferir o influenciar, de cualquier manera en la administración de la Agencia Nacional de Tránsito.

3.1.2.2 Director Ejecutivo de la Agencia Nacional de Tránsito.

Según la Ley Orgánica Reformatoria a la LOTTTSV, el Director Ejecutivo es la máxima autoridad y administrador de la Agencia Nacional de Tránsito, quién es designado por el Directorio de una terna enviada por el Presidente de la República, quiénes deben cumplir requisitos de nacionalidad e idoneidad, conocimiento y experiencia en materia del transporte terrestre, tránsito y seguridad vial [48]. Entre sus funciones y atribuciones se tiene:

- Preparar normas de homologación, regulación y control de equipos y sistemas de transporte y tránsito terrestres, que serán puestas a consideración del Directorio para su aprobación, reforma o delegación;
- Elaborar los reglamentos internos necesarios para el cumplimiento de sus funciones y someterlos a aprobación del Directorio;
- Auspiciar programas, proyectos, actividades y publicaciones objeto de su competencia; y,
- *Aprobar y homologar vehículos automotores, medios y sistemas tecnológicos de transporte terrestre, taxímetros y otros equipos destinados a la regulación del servicio de transporte terrestre*;

3.1.3 NORMATIVA LEGAL

De acuerdo a información provista por el departamento legal de la Agencia Nacional de Tránsito, publicada en su sitio web, la base legal que rige a la ANT se la puede resumir en la Tabla 3.1.3.1.

TIPO DE LA NORMA	NORMA JURÍDICA	REGISTRO OFICIAL No.	FECHA PUBLICACIÓN
Carta Suprema	Constitución de la República del Ecuador	449	20/10/ 2008
Norma internacional	Pacto Internacional de Derechos Civiles y Políticos	101	24/01/1967
	Convención Interamericana sobre Derechos Humanos	801	06/08/1984
Código	Código Orgánico de Coordinación Territorial, Descentralización y Autonomía	303	19/10/2010

Ley Orgánica	Ley Orgánica de Transparencia y Acceso a la Información Pública	337	18/05/ 2004
	Ley Orgánica del Sistema Nacional de Contratación Pública	395	04/08/ 2008
	Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional	52	22710/2009
	Ley Orgánica de Servicio Público	294	06/10/ 2010
	Ley Orgánica de la Contraloría General del Estado	595	12/06/ 2012
	Ley Orgánica del Consejo de Participación Ciudadana y Control Social	22	09/09/2009
	Ley Orgánica de Transporte Terrestre, Tránsito y Seguridad Vial	398	07/08/2008
Reglamentos de Leyes	Reglamento General a la Ley Orgánica de Transparencia y Acceso a la Información Pública	507	19/01/2005
	Reglamento General a la Ley Orgánica del Sistema Nacional de Contratación Pública	588	12/05/2009
	Reglamento a Ley Orgánica de Transporte Terrestre, Tránsito y Seguridad Vial	731	25/06/ 2012
	Reglamento a la Ley Orgánica de Servicio Público	418	01/04/ 2011

Tabla 3.1.3.1: Base legal que rige a la Agencia Nacional de Transito.

Base legal de la Tabla 3.1.3.1, que no contempla la normativa bajo la cual debe regirse la Dirección de Tecnologías de la Información.

3.1.4 SERVICIOS INSTITUCIONALES

La Agencia Nacional de Tránsito, en su calidad de entidad pública al servicio de la ciudadanía ecuatoriana en el ámbito de su competencia, provee de los siguientes servicios ciudadanos descritos en la Tabla 3.1.4.1. [50]

N.	DENOMINACIÓN DEL SERVICIO	DESCRIPCIÓN DEL SERVICIO	COSTO	BENEFICIARIOS/USUARIOS	OFICINAS Y DEPENDENCIAS QUE OFRECEN EL SERVICIO
1	Solicitud de Acceso a la Información Pública	Listado de las instituciones que conforman la Función Ejecutiva años 2011, 2012 y 2013	Gratuito	Ciudadanía en general	A nivel nacional
2	Autorización de funcionamiento para la empresa de renta de vehículos.	Autorización emitida por parte de la Agencia Nacional de Tránsito para el funcionamiento de la empresa de renta de vehículos.	$30	Personas jurídicas	ANT Matriz
3	Habilitación de vehículos para la empresa de renta de vehículos.	Se procede a la habilitación de los vehículos para que pertenezcan como vehículos de renta.	$10 /vehículo	Personas jurídicas	ANT Matriz
4			$10		ANT Matriz

	Deshabilitación de vehículos para la empresa de renta de vehículos.	Se procede a la des-habilitación de los vehículos para que dejen de pertenecer como vehículos de renta.	/vehículo	Personas jurídicas	
5	Concesión de contrato de operación para transporte público en pasajeros interprovincial	Autorización emitida por la Agencia Nacional de Tránsito para que la compañía o empresa pueda formar parte del transporte interprovincial en el territorio Ecuatoriano.	$200	Personas jurídicas	ANT Matriz
6	Habilitación de vehículos para transporte público en pasajeros interprovincial.	Es el documento habilitante que emite la ANT, para que un vehículo pueda ingresar al servicio público, es decir legalizar su unidad y obtener los respectivos beneficios en la exoneración de matrícula en el SRI.	$10	Personas jurídicas	ANT Matriz
7	Deshabilitación de vehículos para transporte público en pasajeros interprovincial.	Emisión de título habilitante para que un vehículo deje de pertenecer a una compañía u operadora de transporte.	$10	Personas jurídicas	ANT Matriz
8	Cambio de socio para transporte público en pasajeros interprovincial.	La resolución de cambio de socio, es el documento habilitante que emite la ANT, para que un socio deje de pertenecer a una compañía o cooperativa e ingrese un nuevo socio transfiriéndose el mismo vehículo.	$10	Personas jurídicas	ANT Matriz
9	Cambio de vehículo para transporte público en pasajeros interprovincial.	Emisión de título habilitante donde el vehículo que consta con el socio, va ser remplazado por otra unidad con mínimo un año posterior a la fabricación del vehículo saliente, para así tener un mejoramiento de flota vehicular.	$10	Personas jurídicas	ANT Matriz
10	Cambio de socio y vehículo para transporte público en pasajeros interprovincial.	Emisión de título habilitante cuando un socio con su vehículo dejan de pertenecer a una compañía o cooperativa, e ingresa un nuevo socio con su propio vehículo.	$10	Personas jurídicas	ANT Matriz
11			$10		ANT Matriz

	Cambio de socio con habilitación para transporte público en pasajeros interprovincial.	La resolución de cambio de socio y habilitación es el documento habilitante que emite la ANT para que el socio que constaba con el cupo pendiente deje de pertenecer a una compañía o cooperativa e ingresa un nuevo socio habilitando su propia unidad.		Personas jurídicas	
12	Autorización para constitución jurídica para transporte público en pasajeros interprovincial.	Resolución previa al contrato de operación.	$145	Personas jurídicas	ANT Matriz
13	Autorización para constitución jurídica para transporte comercial de pasajeros modalidad turismo	Resolución previa al permiso de operación.	$145	Personas jurídicas	ANT Matriz
14	Concesión del permiso de operación para transporte comercial de pasajeros modalidad turismo	Autorización emitida por la Agencia Nacional de Tránsito para que la compañía pueda llevar turistas a nivel nacional.	$200	Personas jurídicas	ANT Matriz
15	Renovación del permiso de operación para transporte comercial de pasajeros modalidad turismo	Autorización emitida por la Agencia Nacional de Tránsito para que la compañía continúe con sus funciones transportando pasajeros que realizan turismo a nivel nacional.	$200	Personas jurídicas	ANT Matriz
16	Incremento de cupo para transporte comercial de pasajeros modalidad turismo	Autorización emitida por la Agencia Nacional de Tránsito para que la compañía pueda obtener 3 cupos más	$200	Personas jurídicas	ANT Matriz
17	Habilitación de vehículos para transporte comercial de pasajeros modalidad turismo	Es el documento habilitante que emite la ANT, para que un vehículo pueda ingresar al servicio público, es decir legalizar su unidad y obtener los respectivos beneficios en la exoneración de matrícula en el SRI.	$10	Personas jurídicas	ANT Matriz
18	Deshabilitación de vehículos para transporte comercial de pasajeros modalidad turismo	Emisión de título habilitante para que un vehículo deje de pertenecer a una operadora de transporte.	$10	Personas jurídicas	ANT Matriz

19	Cambio de Socio para transporte comercial de pasajeros modalidad turismo	La resolución de cambio de socio, es el documento habilitante que emite la ANT, para que un socio deje de pertenecer a una compañía e ingrese como socio la misma compañía transfiriéndose el mismo vehículo.	$10	Personas jurídicas	ANT Matriz
20	Cambio de vehículo para transporte comercial de pasajeros modalidad turismo	Emisión de título habilitante donde el vehículo que consta con el socio, va ser remplazado por otra unidad con mínimo un año posterior a la fabricación del vehículo saliente, para así tener un mejoramiento de flota vehicular.	$10	Personas jurídicas	ANT Matriz
21	Ingreso de documentación	Se recepta el documento que ingresa el usuario.	Gratuito	Ciudadanía en general	ANT Matriz
22	Certificados	Título habilitante que emite la ANT, donde se certifica la veracidad del documento según el sistema que maneja la ANT. Existen certificados de: licencia, matrícula, gravamen, historial vehicular, propiedad vehicular, récord de infracciones	$7.00	Ciudadanía en general	A nivel nacional.
23	Ficha de licencia	Documento que solicita el usuario que tiene licencia tipo c en adelante para respaldar la veracidad y poder realizar trámites como; renovación de licencia, actualización de datos de licencia.	Gratuito	Ciudadanía en general	ANT Matriz
24	Origen vehicular	Se entregan los documentos desde que el vehículo fue registrado en la ANT.	Gratuito		ANT Matriz
25	Actualización de datos de matrícula	Se actualizan los datos erróneos de una matrícula en el sistema, excepto cilindraje.	Gratuito		ANT Matriz
26	Actualización de datos de licencia	Se actualizan los datos erróneos de una licencia.	Gratuito	Ciudadanía en general	ANT Matriz
27	Actualización gravamen	Se procede a levantar o a colocar un gravamen al vehículo según el caso	$7	Ciudadanía en general	ANT Matriz

Tabla 3.1.4.1: Servicios Institucionales que provee la Agencia Nacional de Tránsito.

Información de la Tabla 3.1.4.1, a la que se debe incorporar servicios relacionados con procesos de matriculación, licencias, *homologación de dispositivos* y vehículos, chatarrización, permisos internacionales, transporte seguro y sistema recaudo [50].

3.1.5 CARACTERIZACIÓN DE LA DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

La Agencia Nacional de Tránsito al formar parte del Gobierno Central, se encuentra sujeta a los planes y programas emanados por el Gobierno en todo lo referente a Gobernabilidad Electrónica, siendo responsabilidad de la Dirección de Tecnologías de la Información, garantizar tal disposición, de conformidad al Estatuto Orgánico de Gestión Organizacional por Procesos [49].

3.1.5.1 Misión

La misión de la Dirección de Tecnologías de la Información y Comunicaciones es "Velar por la operación de la ANT, brindando: asesoría, servicios, soporte y administración de la infraestructura tecnológica, con una política de altos estándares de calidad; contribuyendo de esta manera con las estrategias y la misión de la organización"

3.1.5.2 Atribuciones y Responsabilidades

La Dirección de Tecnologías de la Información y Comunicaciones, tiene equipos técnicos de trabajo, distribuidos en sus unidades administrativas esquematizadas en la Figura 3.1.5.1, para el desarrollo de las siguientes atribuciones y responsabilidades [49]:

- Asesorar al nivel directivo en el uso de nuevas tecnologías de información y comunicaciones para innovar los procesos organizacionales.
- Proponer los términos de referencia y pliegos concernientes a la contratación de las tecnologías de la información y comunicaciones.
- Dirigir el diseño, planificación e implementación de proyectos de tecnologías de información y comunicaciones.
- Administrar y monitorear el uso de recursos tecnológicos que dispone la ANT: hardware, software y comunicaciones.

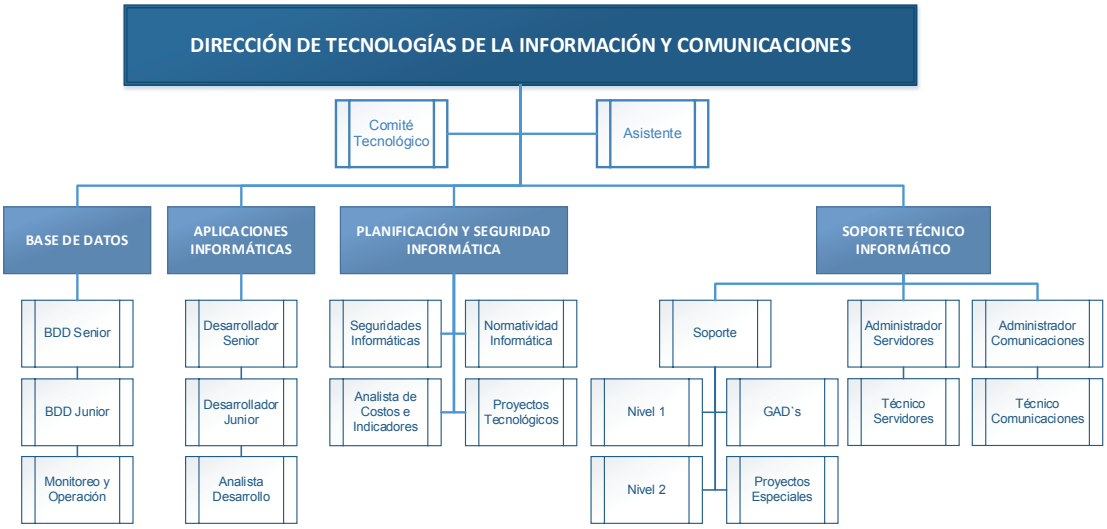

Figura 3.1.5.1 Orgánico Funcional Dirección de Tecnologías de la Información [49].

3.1.5.3 Reglamentación y/o Base Legal

La Dirección de Tecnologías de la Información y Comunicaciones, en su calidad de Proceso Habilitante de Apoyo a la gestión y consecución de objetivos y metas institucionales de los Procesos Gobernantes y Procesos Agregadores de Valor, se fundamenta en la siguiente normativa legal [51], que se resume en la Tabla 3.1.5.1:

- Acuerdo Ministerial 1002 – Norma Técnica de Implementación y Operación de la Metodología y Herramienta De Gobierno Por Resultados, que establece los lineamientos para obtener una gestión pública de calidad, orientada a resultados, centrada en el ciudadano y fundamentada en los principios de Administración Pública establecidos en la Constitución de la República, así también dar, transparencia y continuidad a la gestión de las instituciones públicas mediante la definición, alineación, seguimiento y actualización de sus planes estratégicos, planes operativos, riesgos, proyectos y procesos [52].

- Acuerdo Ministerial 1580 – Norma Técnica de Administración por Procesos, que establece los lineamientos generales para la administración por procesos en las instituciones de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva, a fin de mejorar la eficacia y eficiencia de sus operaciones que aseguren la provisión de servicios y productos de calidad centrados en el ciudadano, acorde con los principios de Administración Pública establecidos en la Constitución de la República [53].

- Acuerdo Ministerial 718 – Instructivo para Normar el Uso del Sistema de Gestión Documental Quipux, en las Entidades de la Administración Publica, que permite desarrollar la gestión documental del sector público mediante la incorporación de Tecnologías de Información y Comunicación, para agilitar el flujo de información y la correspondencia interna, así como entre entidades públicas, bajo estrictas normas y estándares de seguridad, confidencialidad, privacidad, disponibilidad y conservación de la información [54].

- Acuerdo Ministerial 1062 – Norma Técnica de Interoperabilidad Gubernamental, que establece los lineamientos para desarrollar la política pública de Interoperabilidad Gubernamental en la Administración Pública Central, Institucional y Dependiente de la Función Ejecutiva (APCID) [55], con la que se pretende mejorar la coordinación gubernamental, facilitar la generación de insumos para la toma de decisiones, favorecer el uso más racional de los recursos públicos, facilitar los servicios entregados a los ciudadanos e intensificar el intercambio de datos e información electrónica, aplicando normas, procedimientos y estándares abiertos y comunes en la Administración Pública.

- Ley 67 – Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, mediante el cual se regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas [56].

- Ley Orgánica de Transporte Terrestre Tránsito y Seguridad Vial, mediante el cual, se organiza, planifica, fomenta, regula, moderniza y controla el Transporte Terrestre, Tránsito y Seguridad Vial, con el fin de proteger a las personas y bienes que se trasladan de un lugar a otro por la red vial del territorio ecuatoriano, y a las personas y lugares expuestos a las contingencias de dicho desplazamiento, contribuyendo al desarrollo socio-económico del país en aras de lograr el bienestar general de los ciudadanos [48], y

- Estatuto Orgánico de Gestión Organizacional por Procesos de la Agencia Nacional de Regulación y Control del Transporte Terrestre, Tránsito y Seguridad Vial [49].

TIPO DE LA NORMA	NORMA JURÍDICA	REGISTRO OFICIAL No.	FECHA PUBLICACIÓN/ REFORMA
Acuerdo Ministerial	Norma Técnica de Implementación y Operación de la Metodología y Herramienta De Gobierno Por Resultados	606	28/12/2011
Acuerdo Ministerial	Norma Técnica de Administración por Procesos.	895	20/02/2013
Acuerdo Ministerial	Instructivo para Normar el Uso del Sistema de Gestión Documental Quipux en las Entidades de la Administración Publica	597	27/07/2011
Acuerdo Ministerial	Norma Técnica de Interoperabilidad Gubernamental	467	26/03/2015
Ley Orgánica	Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos	557	10/02/2014
Ley Orgánica	Ley Orgánica de Transparencia y Acceso a la Información Pública	337	18/05/ 2004
Reglamento de Ley	Reglamento Orgánico Por Procesos de la Agencia Nacional de Transito	323	27/06/2012

Tabla 3.1.5.1: Base legal que rige a la DTIC – ANT

3.1.5.4 Proyectos e Innovación Tecnológica.

La Dirección de Tecnologías de la Información y Comunicaciones, para el cumplimento de su misión, atribuciones y responsabilidades ha ejecutado y se encuentra ejecutando los siguientes proyectos tecnológicos:

- **Contrato 5497218-CNT**

  Contratación de Servicios Portadores: Enlace de Datos, Internet, GPRS, Telefonía Móvil, Internet Móvil.

  - ***Fecha suscripción***: 01 de septiembre de 2010
  - ***Costo Referencial***: USD $ 78.319,14 mensuales
  - ***Soporte y Mantenimiento***: Vigente
  - ***Objetivo***: Proveer a la Agencia Nacional de Tránsito del Servicio de Portadores (Enlace de Datos, Internet y GPRS), de forma contínua y permanente, garantizando la confidencialidad y seguridad de la información que circule por ella hacia las diferentes dependencias internas y externas, salvo solicitud de la autoridad competente, pero regida por la legislación ecuatoriana. El servicio requerido debe cumplir con disponibilidad mínima mensual de 99.6%; calidad del servicio medido por retardos menores a

120ms y una tasa de error de bit inferior a $1x10^{-8}$ (BER); centro de servicio técnico 7x24x365; Tiempo Promedio de Recuperación de 03h00 (99,6%).

- ***Bienes y/o servicios***:

PROVINCIA	CIUDAD	DEPENDENCIA	TIPO ENLACE	TECNO.	AB (MBPS)
Azuay	Cuenca	ANT Dirección Provincial + Agencia Azuay	DATOS	F.O.	3
Cañar	Azogues	ANT Agencia Azogues	DATOS	F.O.	3
Chimborazo	Riobamba	ANT Agencia Riobamba	DATOS	F.O.	3
Guayas	Zamborondón	ANT Dirección Provincial + Agencia Guayas	DATOS	F.O.	3
Guayas	Guayaquil	ANT Registro Civil Agencia Sur	DATOS	F.O.	3
Guayas	Guayaquil	ANT Registro Civil Norte	DATOS	F.O.	3
Guayas	Guayaquil	ANT - Transporte Seguro CIS	GPRS	F.O.	50
Guayas	Guayaquil	Transporte Seguro Puntilla Mall	Internet	F.O.	45
Guayas	Guayaquil	Transporte Seguro	Internet	F.O.	60
Pichincha	Matriz	ANT – EPMMOP	DATOS	F.O.	3
Pichincha	Matriz	ANT - MUNICIPIO QUITO	DATOS	F.O.	5
Pichincha	Matriz	ANT - Transporte Seguro	DATOS	F.O.	10
Pichincha	Matriz	ANT – DINACOM	DATOS	F.O.	10
Pichincha	Matriz	ANT - Data Center CNT BK	DATOS	F.O.	20
Pichincha	Matriz	ANT – INTERMINISTERIAL	DATOS	F.O.	20
Pichincha	Matriz	ANT - Data Center CNT Principal	DATOS	F.O.	40
Pichincha	Matriz	ANT Cuarto de Monitoreo	Internet	F.O.	5
Pichincha	Matriz	ANT Matriz Backup	Internet	F.O.	5
Pichincha	Matriz	ANT – INTERMINISTERIAL	Internet	F.O.	10
Pichincha	Matriz	ANT Matriz Principal	Internet	F.O.	40
Pichincha	Matriz	ANT – CTE	TUNEL IP	F.O.	10
Tungurahua	Ambato	ANT Agencia Ambato	DATOS	F.O.	3

Tabla 3.1.5.2: Principales Servicios Portadores.

- **Contrato 092-DAJ-CNTTTSV-2010**

Adquisición de infraestructura tecnológica (servidores blade tipo a, b, c, d, fuentes de poder, racks, sistemas de unidad de almacenamiento, librerías de respaldo) necesarias para el procesamiento, almacenamiento, respaldo y demás derivados para el uso y funcionamiento de los sistemas de información de la Comisión Nacional de Transporte Terrestre, Tránsito y Seguridad Vial – CNTTTSV.

- ***Fecha suscripción***: 07 de diciembre de 2010
- ***Costo Referencial***: USD $ 556.000,00
- ***Soporte y Mantenimiento***: Vigente

- ***Objetivo***: Contar con la información nacional de tránsito para poder brindar un servicio ágil, eficiente y seguro a toda la ciudadanía en las diferentes dependencias de tránsito a nivel nacional, para que exista una integración de las bases de datos, contar con las licencias respectivas para la base de datos institucional y

- Dotar a la Agencia Nacional de Tránsito de equipos que permitan y aseguren el procesamiento, almacenamiento y respaldo de la información de tránsito que se maneja en cada una de sus dependencias a nivel nacional de manera óptima y efectiva, en respuesta al Convenio de Cooperación Interinstitucional suscrito con la Comisión de Tránsito del Guayas – CTG, y el Convenio Marco de Transferencia de Tecnología con la Policía Nacional del Ecuador – PNE. Lo que a su vez permitirá a la ANT brindar un servicio ágil, eficiente y seguro a toda la ciudadanía

- ***Bienes y/o servicios***:

PARTE N.	DESCRIPCIÓN	CANT	OBSERV.	TIPO	MOD
93084PX	IBM 42U Enterprise Rack	1	Hardware	9308	RC4
88524TU	IBM eServer BladeCenter(tm) H Chassis with 2x2900W PSU	1	Hardware	8852	HC1
7870H2U	HS22, Xeon 6C X5650 95W 2.66GHz/1333MHz/12MB, 3x2GB, O/Bay 2.5in SAS	4	Hardware	7870	AC1
1746A4D	IBM System Storage DS3524 Express Dual Controller Storage System	1	Hardware	1746	C4A
49Y1841	146GB 2.5in 15K 6Gb SAS HDD	16	Hardware		
172642X	IBM System Storage DS3400 Dual Controller	1	Hardware	1726	HC4
44W2239	IBM 450GB 3.5in HS 15K SAS HDD	12	Hardware		
172701X	IBM System Storage EXP3000	2	Hardware	1727	HC1
43X0802	Express IBM 300GB 3.5in 15K HS SAS HDD	22	Hardware		
249824E	Express IBM System Storage SAN24B-4	2	Hardware	2498	B24
35734UL	TS3200 Tape Library Model L4U Driveless	1	Hardware	3573	L4U
95P5004	Ultrium 4 Fibre Channel Drive	2	Hardware		
95P4278	Ultrium 4 Data Cartridges (5 pack)	4	Hardware		
840670Y	Blade Sever Power PS700	2	Hardware	8406	70Y
8205E6B	IBM Power 740 Express	1	Hardware	8205	E6B
5639RHL	Red Hat Enterprise Linux For Power	1	Software	5639	RHL
5692A6P	AIX System Software POWER	4	Software	5692	A6P
5765AVE	IBM PowerVM Lx86 for x86 Linux	1	Software	5765	AVE
5765G62	AIX 6 for POWER V6.1	3	Software	5765	G62
5765PVS	PowerVM Standard Edition	1	Software	5765	PVS

5765AVE	IBM PowerVM Lx86 for x86 Linux	2	Software	5765	AVE
5692LOP	SPO for Linux on POWER	1	Software	5692	LOP

Tabla 3.1.5.3: Adquisición de servidores, sistema de almacenamiento y respaldos.

- **Contrato 058-DE-DCP-ANT-2012**

  Contratación de los servicios especializados para la adquisición de un Sistema Único Integrado de Tránsito a Nivel Nacional.

  - ***Fecha suscripción***: 13 de diciembre de 2012
  - ***Costo Referencial***: USD $ 1 127.510,97
  - ***Soporte y Mantenimiento***: Vigente
  - ***Objetivo***: Dotar a la Agencia Nacional de Tránsito de un Único Sistema Nacional de Tránsito que permita la desconcentración y descentralización de los servicios y procesos de acuerdo a lo establecido en la Ley Orgánica del Transporte Terrestre tránsito y Seguridad Vial.
  - ***Bienes y/o servicios***:

No.	DESCRIPCIÓN	CANT	OBSERV	TIPO	MOD
1	Diagnóstico de Seguridades existentes en las Tecnologías de la Información.	1	Servicios		
2	Definición de la Base de Datos Unificada.	1	Servicios		
3	Implementación de la Base de Datos Unificada.	1	Servicios		
4	Definición de Procesos de Control de Cartera, Control de Ingresos e Interfaz Contable.	1	Servicios		
5	Implementación de Procesos de Control de Cartera, Control de Ingresos e Interfaz Contable en la BD Unificada.	1	Servicios		
6	Diagnóstico de los Procesos de Tránsito.	1	Servicios		
7	Definición del nuevo Modelo de Gestión de los Procesos de Tránsito.	1	Servicios		
8	Implementación del nuevo Modelo de Gestión de los Procesos de Tránsito sobre la Base de Datos Unificada.	1	Servicios		
9	Sistema de Indicadores de los Procesos de Tránsito.	1	Servicios		
10	Transferencia del Conocimiento.	1	Servicios		
11	Database Enterprise Edition	56	Software		
12	Real Application Cluster	56	Software		
13	Tuning Pack	6	Software		

14	Diagnostic Pack	6	Software		
15	Database Vault	6	Software		
16	Advanced Security	6	Software		
17	Lifecycle Management Pack	6	Software		
18	Web Logic Suite	54	Software		
19	Internet Developer Suite	5	Software		
20	IBM System x3550 M4	2	Hardware	7914	AC1
21	Oracle Data Base	1	Hardware		
22	HS23, Xeon 4C E5-2609 80 W 2.40GHz/1066MHz/10MB, 4x4GB, O/Bay 2.5in SAS	1	Hardware	7875	AC1

Tabla 3.1.5.4: Adquisición Sistema Unificado de Transito AXIS 4.0

- **Contrato 059-DE-DCP-ANT-2012**

  Adecuación del Cuarto de Comunicaciones y Cuarto de UPS del Edificio Matriz de la Agencia Nacional de Tránsito.

  - ***Fecha suscripción***: 13 de diciembre de 2012
  - ***Costo Referencial***: USD $ 227.999,81
  - ***Soporte y Mantenimiento***: Vigente
  - ***Objetivo***: Dotar a la Agencia Nacional de Tránsito de equipamiento tecnológico para el funcionamiento del Cuarto de Comunicaciones y Cuarto de UPS del edificio Matriz, a fin garantizar óptimas condiciones de climatización, seguridad, gestión y monitoreo para el funcionamiento de los equipos activos de comunicación y servidores.
  - ***Bienes y/o servicios***:

No.	DESCRIPCIÓN	CANT	OBSERV
1	UPS EATON 9390 80/80 KVA	2	Hardware
2	Evaporadora York 48000 BTU	1	Hardware
3	Condensadora York 48000 BTU	1	Hardware
4	Evaporadora CANATAL 6ADOS	1	Hardware
5	Condensadora CANATAL KS11-078-1	1	Hardware
6	Sistema racks	1	Hardware
7	Control de acceso	2	Hardware
8	Tableros de distribución	1	Servicios
9	Red eléctrica	1	Servicios
10	Cableado estructurado	1	Servicios
11	Sistema de piso de acceso elevado	1	Servicios
12	Malla de alta frecuencia	1	Servicios

13	Pintura antiestática	1	Servicios
14	Puerta de seguridad	1	Servicios
15	Sistema de detección y extinción de incendios	1	Servicios
16	Adecuaciones fiscas para las dos áreas a adecuar	1	Servicios
17	Traslado sistema de seguridad y video	1	Servicios

Tabla 3.1.5.5: Centro de Datos y UPS para el Edificio Matriz.

- **Contrato 034-DE-DCP-ANT-2013**

  Adquisición, instalación y puesta en servicio de un sistema de Recaudo integrado para el sistema de transporte público urbano de los cantones de Santa Elena, Libertad y Salinas, en la provincia de Santa Elena.

  - ***Fecha suscripción***: 12 de agosto de 2013
  - ***Costo Referencial***: USD $ 3´892.354,00
  - ***Soporte y Mantenimiento***: Vigente
  - ***Objetivo***: Dar cumplimiento a lo dispuesto en la Ley Orgánica del Transporte Terrestre Transito y Seguridad Vial, respecto a "fomentar el principio de gestión empresarial por parte de las operadoras de transporte terrestre, sustentado en las bondades que las Tecnologías de la Información y Comunicación – TIC´s – provee"
  - ***Bienes y/o servicios***:

No.	DESCRIPCIÓN	CANT	OBSERV
1	Kit Equipamiento Autobuses	240	Hardware
2	Red de Recargas Tiendas	110	Hardware
3	Equipamiento para credencialización	6	Hardware
4	Equipamiento para recarga y expendio automático	10	Hardware
5	Sistema Central: Servidores, Telecomunicaciones y Sistema Base	1	Hardware
7	Tarjetas sin contacto	175000	Hardware
8	Mantenimiento, soporte y transferencia de conocimientos.	1	Servicios

Tabla 3.1.5.6: Sistema Recaudo para la provincia de Santa Elena.

- **Contrato CNT 2013-ANT**

  Contratación de Servicio de Housing.

  - ***Fecha suscripción***: 01 de septiembre de 2013

- ***Costo Referencial***: USD $ 1.080,00 mensuales
- ***Soporte y Mantenimiento***: Vigente
- ***Objetivo***: Proveer a la Agencia Nacional de Tránsito el Servicio de Housing para la instalación y configuración de la infraestructura tecnológica (3 racks) en un Centro de Datos que cumpla con las normas EIA/TIA – 942 (TIER II), para aumentar la redundancia y los niveles de confiabilidad y minimizar puntos únicos de falla proveyendo un porcentaje de disponibilidad del 99,741%. La solución, incluye: Sistema de Control de Acceso (huella digital y/o tarjeta inteligente); Sistema de Aire Acondicionado de Precisión Redúndate; Sistema de Detección y Extinción de Incendios; Sistema de UPS redundantes; Sistema de Video Vigilancia; Espacio para ubicar 3 racks de 42UR; Piso y Techo Falso, Centro de Monitoreo 24/7, enlace de Internet de 6 Megas o por la misma capacidad entre el Data Center y la Entidad Contratante.
- ***Bienes y/o servicios***:

NO.	DESCRIPCIÓN	CANT.	OBSERV.
1	Servicio mensual de Housing en el centro de Datos de la Corporación Nacional de Telecomunicaciones – CNT EP, Gaspar de Villarroel y Jorge Drom.	1	Servicios

Tabla 3.1.5.7: Servicio de Housing TIER II

- **Contrato 050-DE-DCP-ANT-2013**

  Adquisición e instalación de equipos de seguridad perimetral y protección de correo electrónico para la Agencia Nacional de Tránsito

  - ***Fecha suscripción***: 08 de octubre de 2013
  - ***Costo Referencial***: USD $ 475.216,00
  - ***Soporte y Mantenimiento***: Vigente
  - ***Objetivo***: Reforzar la seguridad de la información de la Agencia Nacional de Transito mediante un mecanismo de seguridad perimetral que permita brindar la garantía de protección contra posible ataques provenientes tanto de la red interna como externa (internet, WAN), dado el crecimiento permanente e innovación tecnológica de la Institución. Entre otras cosas, la solución debe evitar y prevenir ataques informáticos externos al reforzar el esquema de seguridades perimetral: firewall, VPN, cifrado, inscripción,

AntiSpam, monitoreo y generación de reportes; capacitar al personal técnico de la ANT en la administración y operación de la plataforma a implementar; solventar las recomendaciones realizadas por entidades auditoras.

- ***Bienes y/o servicios***:

No.	DESCRIPCIÓN	CANT	OBSERV
1	Equipos de Seguridad Informática "Fortigate 3040B"	2	Hardware
2	Equipo de Análisis y Almacenamiento de Log's "FortiAnalyzer 2000B"	1	Hardware
3	Equipos de Protección de Correo Electrónico "FortiMail 400C"	2	Hardware
4	Instalación, configuración y transferencia de conocimiento.	1	Servicios

Tabla 3.1.5.8: Seguridad Perimetral y Anti Spam.

- **Contrato 051-DE-DCP-ANT-2014**

Renovación de licencias de software antivirus a nivel nacional

- ***Fecha suscripción***: 07 de octubre de 2014
- ***Costo Referencial***: USD $ 21.529,50
- ***Soporte y Mantenimiento***: Vigente
- ***Objetivo***: Dotar a la Agencia Nacional de Tránsito de una solución de protección de antivirus a fin de dar continuidad y seguridad informática a los servidores, computadoras de escritorio y/o portátiles, red de datos y aplicativos.
- ***Bienes y/o servicios***:

No.	PRODUCTO	CAN.	OBSERV.
1	Licencias Kaspersky Endpoint Security Business Select (por 3 años).	1.000	Software

Tabla 3.1.5.9: Antivirus Corporativo a nivel nacional.

- **Contrato 053-DE-DCP-ANT-2014**

Infraestructura de comunicaciones para el mejoramiento de la red a nivel nacional

- ***Fecha suscripción***: 14 de octubre de 2014
- ***Costo Referencial***: USD $ 1'149.580,54
- ***Soporte y Mantenimiento***: Vigente

- ***Objetivo***: Dotar al edificio Matriz y Oficinas de Atención a Usuarios de la Agencia Nacional de Transito a nivel nacional, de tecnología de punta que permita incrementar la disponibilidad de los servicios mediante la implementación de equipos de Networking. En el caso del edificio Matriz, permitirá implementar una plataforma de administración de políticas de seguridad; un gestor para la administración centralizada de la red inalámbrica; y un de ruteo para la configuración QoS y levantamiento de interfaces tipo túnel hacia los router de las agencias, garantizando el cumplimiento total de las normas de control interno, administración del riesgo operativo y las recomendaciones de las auditorías (interna, externa e instituciones).

- ***Bienes y/o servicios***:

No.	DESCRIPCIÓN DEL BIEN	CANTIDAD	OBSERV
1	Switches de Core	2	Hardware
2	Switch de Distribución	1	Hardware
3	Switches de 48 puertos	6	Hardware
4	Switches de 24 puertos	60	Hardware
5	Router de gestión de enlaces	1	Hardware
6	Controladora de Access Points	1	Hardware
7	Access Points	65	Hardware
8	Equipo de seguridad interna	1	Hardware
9	Licencias equipos finales de la solución de seguridad interna x 3 años de suscripción (Paquete de 500 licencias)	3	Servicios
10	Servicio de Instalación (equipos de networking, Wireless, ISE para 500 usuarios)	1	Servicios
11	Mantenimiento preventivo y correctivo anual	3	Servicios
12	Soporte Técnico anual	3	Servicios

Tabla 3.1.5.10: Equipos de Enrutamiento, switch core y sistema de gestión de identidad ISE

- **Contrato 058-DE-DCP-ANT-2014**

  Implementación de una solución para fortalecer el servicio de correo electrónico para disponer de correo seguro y envío de correo masivo

  - ***Fecha suscripción***: 05 de noviembre de 2014
  - ***Costo Referencial***: USD $ 167.912,50
  - ***Soporte y Mantenimiento***: Vigente

- ***Objetivo***: Dotar a la Agencia Nacional de Tránsito de una solución informática que permita fortalecer los pilares de Seguridad Informática en cuanto a Confiabilidad, Integridad y Disponibilidad del servicio de correo electrónico institucional. Entre otras cosas, la solución debe evitar la generación de SPAM o caer en lista negras por envió de correo masivo, incrementar cuentas de correo electrónica con licenciamiento perpetuo e incremento de la seguridad mediante el uso de certificados digitales e encriptación de correo electrónico.

- ***Bienes y/o servicios***:

No.	Descripción del Bien o Servicio	CANT.	OBSERV
1	Renovación Licenciamiento ZIMBRA 3 Años	1350	Software
2	Nuevas Cuentas de Correo Profesional (250 por paquete)	2	Software
3	Implementación Zimbra Collaboration Suite Multiserver	1	Software
4	ZIMBRA Collaboration suite advantage suscripción perpetua para gobierno 3 años (250 por paquete)	2	Software
5	Soporte y Monitoreo de Plataforma Zimbra 5x8 anual	3	Servicio
6	Software de Administración y Estadísticas (para 1850 usuarios)	1	Software
7	Correo Masivo – Sistema MAILING	1	Software
8	Certificados SSL – Servidor	1	Software
9	Certificados S/MIME – Clientes De Correo	50	Software

Tabla 3.1.5.11: Solución de Correo Electrónico Institucional Seguro

- **Contrato 063-DE-DCP-ANT-2014**

  Adquisición de equipos y componentes para el fortalecimiento de servidores para el centro de datos de la Agencia Nacional de Tránsito.

  - ***Fecha suscripción***: 19 de noviembre de 2014

  - ***Costo Referencial***: USD $ 168.000,00

  - ***Soporte y Mantenimiento***: Vigente

  - ***Objetivo***: Garantizar el adecuado funcionamiento y disponibilidad de los servicios tecnológicos de la Agencia Nacional de Tránsito mediante la adquisición de equipos y componentes de servidores y almacenamiento, que permita alcanzar las metas institucionales de manera eficiente y eficaz optimizando los recursos actuales.

  - ***Bienes y/o servicios***:

Part No.	Descripción	Cant.	OBSERV.
7875C4U	**SERVIDORES TIPO BLADE, CUCHILLAS HS23 -** *"IBM BladeCenter HS23, 8C E5-2670 115W 2.6GHz/1600MHz/20MB, 4x4GB, O/Bay 2.5in SAS".*	3	Hardware
8721A1U	**SOLUCIÓN DE SERVIDORES PARA EDIFICIO MATRIZ (EQUIPOS SERVIDORES) -** "*IBM Flex System Enterprise Chassis with 2x2500W PSU, Rackable*".	1	Hardware
873742U	***Servidor Node o Cuchilla IBM Flex System x240 Compute Node***, Xeon 8C E5-2650v2 95W 2.6GHz/1866MHz/20MB, 8GB, O/Bay 2.5in SA (873742U)	3	Hardware
2072S2C	**SISTEMA DE ALMACENAMIENTO, CON 13 DISCOS DE 900GB 10K 2.5-INCH SAS HDD (DATA ESTORAGE o SERVIDOR DE ALMACENAMIENTO) -** "*IBM Storwize V3700 SFF Dual Control Enclosure*".	1	Hardware
D0Q3XLL	**HERRAMIENTA PARA EL MANEJO DE LA INFRAESTRUCTURA DE ALMACENAMIENTO (PAQUETE INFORMÁTICO) -** "*IBM TIVOLI STORAGE MANAGER SUITE FOR UNIFIED RECOVERY ENTRY TERABYTE (1-100) LICENSE + SW SUBSCRIPTION & SUPPORT 12 MONTH*".	12	Software
	Mantenimiento y soporte anual.	3	Servicios

Tabla 3.1.5.12: Re-potenciamiento de Servidores y Almacenamiento, y Solución de Respaldos.

Inversión tecnológica de los últimos cinco años realizada por la Agencia Nacional de Tránsito, que se la puede resumir en la Tabla 3.1.5.13, y que ha permitido a la Dirección de Tecnologías de la Información y Comunicación cumplir con su misión de generar productos y servicios de apoyo a la gestión de los Procesos Gobernantes y Agregadores de Valor.

CONTRATO	DESCRIPCIÓN	FECHA SUSCRIPCIÓN	PRECIO (USD $)
070-DAJ-CNTTTSV	Contratación de Servicios Portadores: Enlace de Datos, Internet, GPRS, PBX, Tunel IP	01/07/2010	4.542.510,12
092-DAJ-CNTTTSV	Adquisición de infraestructura tecnológica: Servidores blades, Racks, Sistemas de almacenamiento, Librerías de respaldo	07/12/2010	556.000,00
058-DE-DCP-ANT	Adquisición de un Sistema Único Integrado de Tránsito a Nivel Nacional: AXIS4.0, Oracle Database Appliance (ODA) y licenciamiento	13/12/2012	1.127.510,97
059-DE-DCP-ANT	Centro de Datos y Cuarto de UPS del Edificio Matriz: Sistema de Climatización, Sistema de Detección y Extinción de Incendios, Sistemas de Control de Accesos, Sistema de Supervisión de Alarmas y Monitoreo, Sistema de Iluminación, Sistema de Protección contra Transitorios (TVSS), Cableado Estructurado, Sistema de Piso Falso, Sistema de Malla de Alta Frecuencia.	13/12/2012	227.999,81
034-DE-DCP-ANT	Adquisición, instalación y puesta en marcha del sistema Recaudo para el transporte público urbano: Kit Equipamiento Autobuses; Red de Recargas Tiendas; Equipamiento para credencialización; Equipamiento para recarga y expendio automático; Sistema Central: Servidores, Telecomunicaciones y Sistema Base; Tarjetas sin contacto	12/08/2013	3.892.354,00
043-DE-DCP-ANT	Contratación del Servicio de Housing en un Centro de Datos que cumpla con las normas EIA/TIA – 942 (TIER II)	01/09/2013	23.760,00
050-DE-DCP-ANT	Adquisición e instalación de equipos de seguridad perimetral (Firewall, análisis y almacenamiento de logs) y protección de correo electrónico (AntiSpam) para la Agencia Nacional de Tránsito	08/10/2013	475.216,00
051-DE-DCP-ANT	Renovación de licencias de software antivirus a nivel nacional	07/10/2014	21.529,50
053-DE-DCP-ANT	Infraestructura de comunicaciones para el mejoramiento de la red a nivel nacional: Router y Switchs Core, switchs de distribución, Wireless Controller e Identity Services Engine (ISE).	14/10/2014	1.149.580,54
058-DE-DCP-ANT	Fortalecimiento del servicio de correo electrónico institucional: Mailing y certificados SSL y S/MIME	05/11/2014	167.912,50
063-DE-DCP-ANT	Adquisición de equipos y componentes para el fortalecimiento de servidores para el centro de datos de la Agencia Nacional de Tránsito: Equipos Servidores, Sistema de Almacenamiento y Herramienta de Backup Corporativa TSM TIVOLI	19/11/2015	168.000,00
		TOTAL	***12.352.373,44***

Tabla 3.1.5.13: Inversión en TIC's de los últimos cinco años.

Gracias a los proyectos de innovación tecnológica, la Agencia Nacional de Tránsito para la generación de productos y servicios de apoyo, cuenta con dos centros de datos, uno instalado y configurado en el edificio matriz y otro en el sector de Iñaquito en modalidad Housing, ambos diseñados y construidos bajo la norma EIA/TIA942, es decir, cuentan con:

- Sistema de control de accesos biométrico (por huella digital), Figura 3.1.5.2
- Sistema de aire de precisión redundante, Figura 3.1.5.4
- Sistema de extinción de incendios, Figura 3.1.5.3
- Sistema UPS redundante
- Piso y techo falso, techo falso.
- Centro de monitoreo 24/7.

Figura 3.1.5.2 Sistema de Control de Acceso DC ANT – CNT.

Figura 3.1.5.3 Sistema de Detección y Extinción de Incendios DC ANT – CNT.

Figura 3.1.5.4 Sistema de Aire Acondicionado de Precisión DC ANT – CNT.

Figura 3.1.5.5 Racks de Servidores y Telecomunicaciones DC ANT – CNT.

En cada Centro de Datos (DC) se encuentra instalada, configurada y operando en condiciones óptimas de enfriamiento, energización y seguridad física, toda la infraestructura tecnológica de la Agencia Nacional de Tránsito de la Tabla 3.1.5.13, necesaria para la provisión de servicios de Tecnologías de la Información y Comunicación (TIC), tanto a sus Oficinas de Atención al Usuario y Direcciones Provinciales, como a los Gobiernos Autónomos Descentralizados y demás entidades gubernamentales y financieras relacionadas con la planificación, regulación y control del Transporte Terrestre, Tránsito y Seguridad Vial. Entre los sistemas se tiene:

- Sistemas de Seguridad Perimetral: Sophos, FotineGate y FortiMail.
- Sistema y Equipos de Comunicación: SAN Switchs, Router Core, Switch Core, Switch de Distribución, Switch de Acceso, Wireless Control.
- Sistema de Procesamiento o Servidores: PureFlex System, IBM BladeCenter H, IBM Power, HP Proliant Gen 7 y 8
- Sistema de Almacenamiento o Data Storage: Storwize, IBM System Storage,
- Sistema de Respaldos o Backups: IBM Tape Library
- Sistema de registro, análisis y reporte: FortiAnalizer
- Sistema de Base de Datos: Oracle Database Appliance (ODA)

Sistemas operando en alta disponibilidad y redundancia en ambos centros de datos, permitiendo a la Dirección de Tecnologías de la Información y Comunicación el cumplimiento de la normativa legal vigente, garantizando la confidencialidad, integridad y disponibilidad de la Información que maneja la Agencia Nacional de Tránsito. A continuación se resume y esquematiza las especificaciones técnicas, beneficios y configuración actual de los sistemas antes mencionados.

SISTEMA	CAN	MARCA	MODELO	UBI	CARACTERÍSTICAS
Seguridad Perimetral:	1	Sophos	SG525	CNT	***Security Applications***: Firewall, NAT, PPTP & L2TP Remote Access ***Network Protection***: IPSec/SSL VPN & Remote Access, VoIP Security, Advanced Routing, Advanced Networking ***Email Protection***: Antivirus, Antispam, Phishing Protection, Email Encryption, Advanced Networking ***Web Protection***: Spyware Protection, URL Filtering, HTTPS Scanning, Application Control.

					Endpoint Protection: Endpoint Antivirus - Features Antivirus, HIPS, Device Control, and Tamper Protection ***Wireless Protection, Webserver Protection***
	2	FotineGate	3040B	ANT	8 Hardware Accelerated 10-GbE SFP+ Interfaces 10 Hardware Accelerated GbE SFP Interfaces 2 Non-Accelerated 10/100/1000 Interfaces 2xSR SFP Transceivers 4 Fortinet Storage Module (FSM) Expansion Slot 64 GB SSD (1x FSM-064) Local Solid State Disk Storage Included Firewall; Intrusion Prevention; Antivirus / Antispyware; VPN: IPSec/L2TP/PPTP (PKI, IKE, L2TP, PPTP, AES, DES, 3DES, MD5, SHA-1, SHA256, IPSec); VPN SSL (LDAP y RADIUS); WAN Optimization; SSL-Encrypted Traffic Inspection; Endpoint NAC; Data Loss Prevention; Web Filtering; Logging, Reporting & Monitoring; High Availability; Application Control; Virtual Domains; Setup / Configuration Options; Wireless Controller; Networking/Routing; User Authentication Options; High Availability (HA); Traffic Shaping; Intrusion Prevention System (IPS); Data Loss Prevention (DLP); Endpoint Compliance And Control;
	2	FortiMail	400C	CNT	4 10/100/1000 Interfaces (Copper, RJ-45) 2 HDD SAS 1 TB Configured Domains; Recipient-based Policies - Incoming or Outgoing; Antispam, Antivirus, Authentication, and Content Profiles; Email Routing; FortiGuard Antispam; FortiGuard Antispam + Antivirus Flexible Deployment Options; Apply Data Loss Prevention and Identity-Based Encryption; Prevent Phishing and Other Advanced Threats; Identify and Block Spamming Endpoints; No Per-User or Per-Mailbox Pricing
	1	CISCO	ISE	ANT	Equipo Seguridad Interna: 2 Quad-Core 2.4 Ghz; 32 GB 2 HDD, 600 GB 4 GEthernet Business-policy enforcement; Access control; AAA protocols; Device profiling; Device profile feed service; Endpoint protection service; Centralized management; Monitoring and troubleshooting
Equipos de Comunicación:	2	IBM	SAN24B-4	CNT	SAN Switchs de 24 puertos. 16 puertos activados
	2	CISCO	4400 Series	ANT / CNT	Router Core Cisco 4400 Series: ISR NIMs, synchronous serial WAN connections. Iinterfaces use well - known point - to - point WAN protocols such as High - Level Data Link Control (HDLC) and Point – to - Point Protocol (PPP) as well as Frame Relay, offering cost - effective virtualized WAN connections in both point – to - point and point - to – mul tipoint designs. You can mix and match NIMs to tailor cost - effective solutions for common networking solutions for low - and high - density WAN aggregation.
	2	CISCO	Catalyst 4507R+E	ANT / CNT	Switch Core Cisco Catalyst 4507R+E: 12 módulos SFP+ de 10 Gbps a máxima velocidad ***Bandwidth capacity***: up to 848 Gbps switching capacity at 48 Gb per slot. ***Redundant power supplies***: have two bays for the power supplies ***Redundant supervisor engines:*** two dedicated slots for supervisor engines.

					AC and DC power options: Standards compliance:
	1	CISCO	4500X Series	ANT	Switch de Distribución Soporta QoS, ToS y QoS Diffserv; VLAN – IEEE 802.1q; Spanning Tree Protocol – 802.1D 16 módulos SFP+ de 10 Gbps
	6	CISCO	Catalyst 2960X	ANT	Switch de Acceso Cisco Catalyst 2960X 48 GigE PoE 740W, 2x 10G SFP+, LAN Base
	1	CISCO	5500 Series	ANT	Wireless Control: Soporta 500AccessPoints; 7000 Usuarios. ***Compatibilidad***: IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11d, IEEE 802.11h, IEEE 802.11n, 802.11ac wave 1 y wave2 ***Seguridad***: WPA, WPA2-RSN, MD5, HMAC; TLS, PKI, Certificate and CRL Profile. ***Encriptación***: WEP and TKIP-MIC, SSL, TLS, RSA, AES, CCM, CCMP. ***Authentication, Authorization, Accounting:*** IEEE 802.1X, RADIUS.
	60	CISCO	Catalyst 2960X	ANT	Switch de Acceso Cisco Catalyst 2960X24 GigE PoE 370W, 2x 10G SFP+, LAN Base
	65	CISCO	Aironet 3700	ANT	Cisco Aironet 3700i Access Point: Dual-band 2.4 GHz and 5 GHz with 802.11ac Wave 1 support on the integrated 5-GHz radio
Sistema de Procesamiento o Servidores:	1	IBM	PureFlex	CNT	Flex System Enterprise Chasis : 2 Switch SAN 8 GB, 2 Switches Ethernet 1Gb 2 CMM B 3 Flex System x240 Nodos: 2 Xeon 8 Core 2.6 Ghz 128 GB RAM/ 2 HD SAS 300GB 4 Ethernet Port 1 Gb 2 FC Port 8Gb
	1	IBM	Blade Center H	CNT	BladeCenter H 4 Switches Ethernet 2 Switches SAN 4 Fuentes Poder 3 Blades HS22 2 Xeon SixCore 2.66GHz 128 GB RAM / 2 HD SAS 146GB 4 Ethernet Ports / 2 FC Ports 2 Blades HS22 1 Xeon SixCore 2.66GHz 64 GB RAM / 2 HD SAS 146GB 4 Ethernet Ports / 2 FC Ports 2 Blades HS23 2 Xeon 8 Core 2.60GHz 128 GB RAM / 2 HD SAS 146GB 4 Ethernet Ports / 2 FC Ports2 Blade PS700 4-cores 3.5GHz 16 GB RAM / 2 HD SAS 146GB 4 Ethernet Ports / 2 FC Ports
	1	IBM	Blade Center H	ANT	BladeCenter H 4 Switches Ethernet 2 Fuentes Poder 2 Blades HS22 2 Xeon 6 Core 2.66GHz

					128 GB RAM / 2 HD SAS 146GB 4 Ethernet Ports / 2 FC Ports 2 Blades HS23 2 Xeon 8 Core 2.60GHz 128 GB RAM / 2 HD SAS 146GB 4 Ethernet Ports / 2 FC Ports2
	3	HP	Proliant DL380e	ANT	3 HP DL380e (G8) 2 Xeon 6 Core2.4GHz 64GB RAM / 4 HD SATA 1 TB 4 Ethernet Ports
	1	HP	Proliant DL380p	ANT	1 HP DL380p (G8) 2 Xeon 6 Core2.4GHz 64GB RAM / 4 HD SATA 1 TB 4 Ethernet Ports
	1	IBM	Power	CNT	P740 Power7 4-cores 3.5GHz 16GB RAM / 2 HD SAS 146GB 2 Dual FC HBA / 1 Tarjeta gráfica 4 Puertos Ethernet Redundant Power
	2	IBM	x3550 M4	CNT	2 Xeon 4 Cores 2.4 GHz 192 GB RAM / 4 HD SAS 300 GB 4Gigabit/2TenGibabit Ethernet Ports
Sistema de Almacenamiento o Data Storage:		IBM	Storwize V3700	CNT	Storwize V3700: 14 HD SAS 900GB 10K rpm 8GB Cache, Dual Controller, Redundant Power
		IBM	System Storage DS3400	CNT	Storage DS3400 + 2 Expansiones: 22 HD SAS 300GB 15K rpm 13 HD SAS 450GB 15K rpm 1GB Caché / Dual Controller Redundant Power
		IBM	System Storage DS3512	ANT	DS3512 + 1 Expansiones 8 HD SAS 500GB 15K rpm 8 HD SAS 1TB 7.2K rpm 1GB Caché / Dual Controller Redundant Power
		IBM	System Storage DS3524	CNT	Storage DS3524 + 2 Expansión 8 HD SAS 600GB 15K rpm 16 HD SAS 146GB 15K rpm 14 HD SAS 300GB 15K rpm 14 HD SAS 900GB 10K rpm 4 HD SAS 3TB 7.2K rpm 2GB Caché – Dual Controller Redundant Power
Sistema de Respaldos o Backups:		IBM	TS3200	CNT	Tape Library TS3200 2 FC Drive Ultrium4/LTO4 Redundant Power
Sistema de registro, análisis y reporte:	2	FortiAnalizer	2000B	ANT	Quad Core CPU, redundant power, 6x 10/100/1000
Sistema de Base de Datos:	1	Oracle	Oracle Database Appliance (ODA)	CNT	1 Oracle Database Appliance (ODA): 4 Xeon 6 Core 3.0 GHz 192 GB RAM / 24 HD SAS 600 GB/4 HD SSD 300 GB 12 Gigabit/4 TenGibabit Ethernet Ports

Tabla 3.1.5.14: Sistemas y Componentes instalados y operando en el DC de CNT y ANT Matriz.

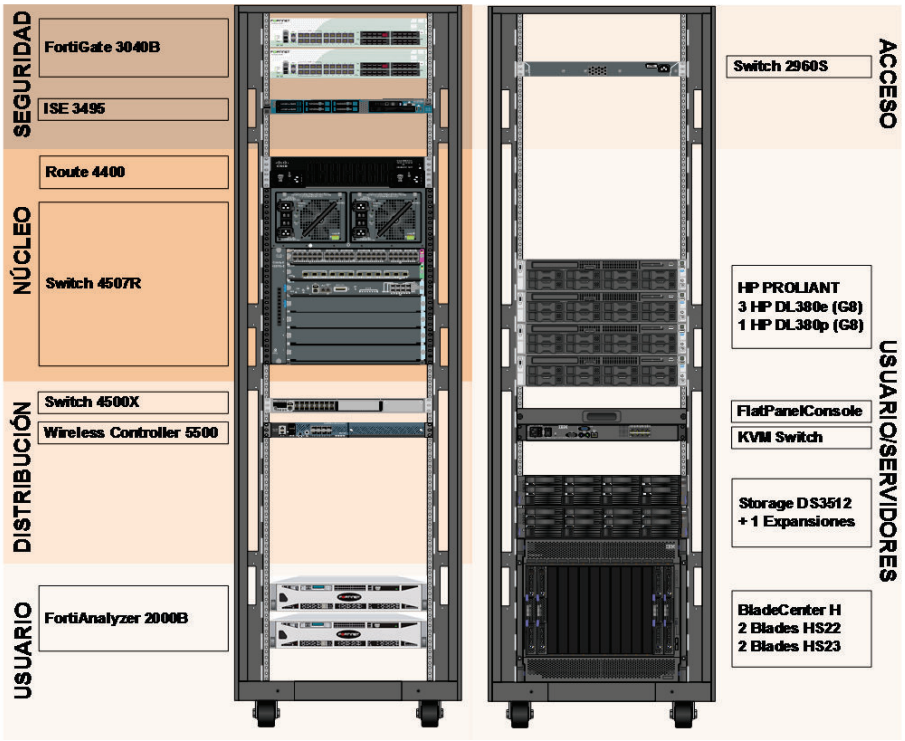

Figura 3.1.5.6 Sistemas y Componentes Centro de Datos ANT

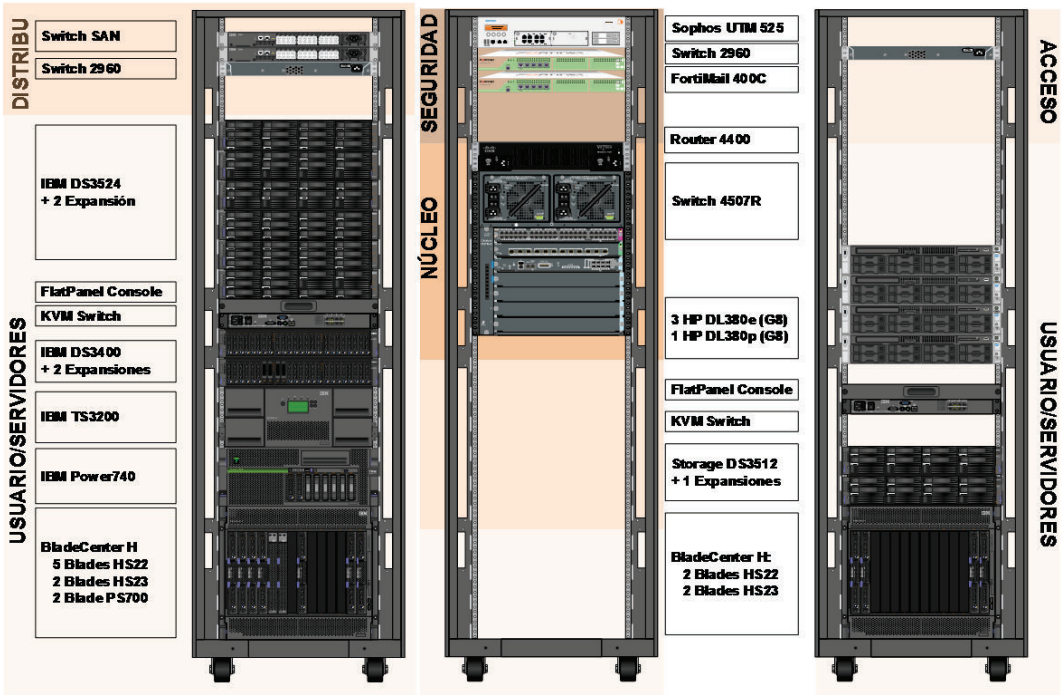

Figura 3.1.5.7 Sistemas y Componentes Centro de Datos CNT – Housing

Sistemas y Componentes del Centro de Datos de las Figura 3.1.5.6 y Figura 3.1.5.7, interconectados entre sí, a través de la red Multi-Protocol Label Switching (MPLS)

de la Corporación Nacional de Telecomunicaciones mediante enlaces de datos e internet redundantes de 40 Mbps (Principal) y 20 Mbps (Backup), lo que garantiza el acceso a los servicios LAN y WAN por parte de las Oficinas de Atención al Usuario, Direcciones Provinciales, Gobiernos Autónomos Descentralizados y demás entidades gubernamentales y financieras, quienes en su mayoría se encuentran interconectados hacia los centros de datos, mediante enlaces punto a punto (Datos) y enlaces de internet de hasta 3Mbps y 2 Mbps respectivamente y por fibra óptica (1:1), como se esquematiza en la Figura 3.1.5.8.

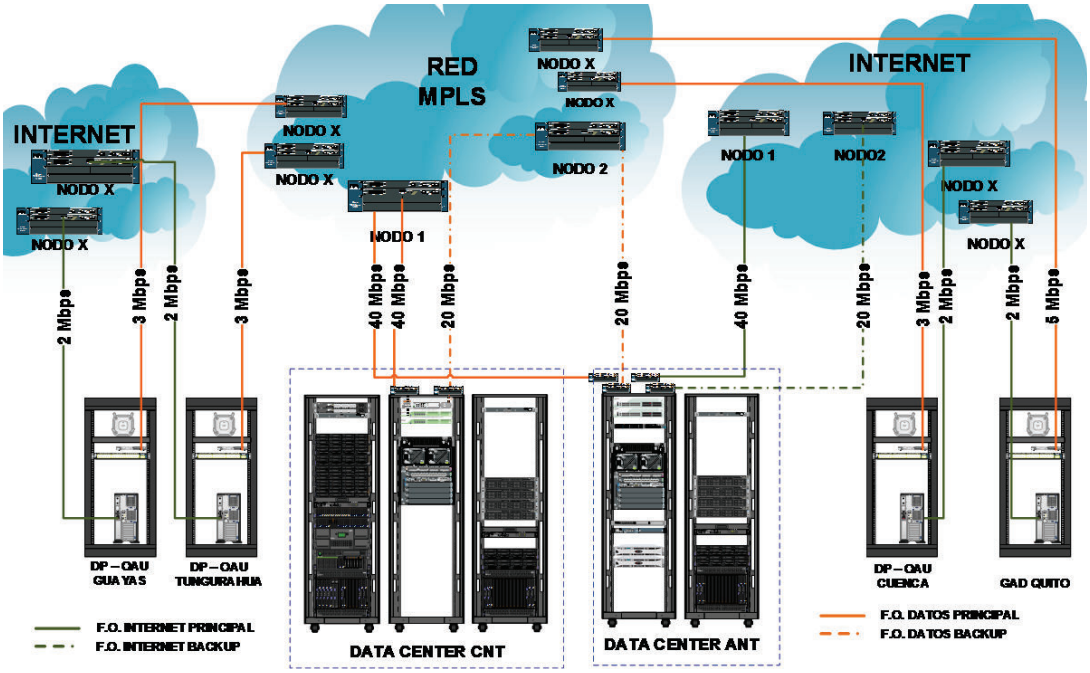

Figura 3.1.5.8 Interconexión LAN y WAN centros de datos y dependencias de la ANT.

Por lo expuesto en esta sección, la Agencia Nacional de Tránsito cuenta con infraestructura de punta con marcas reconocidas en el mercado y posicionadas en los estudios de Gartner que le permiten garantizar los servicios que provee.

3.2 APLICACIÓN DEL MODELO EN LA ENTIDAD CASO DE ESTUDIO.

Considerando que la Innovación Tecnológica del Transporte forma parte del Plan Nacional del Buen Vivir 2013 – 2017 [57], la Agencia Nacional de Tránsito en atribución a la normativa legal vigente que le faculta la “planificación, regulación, modernización y control del Transporte Terrestre, Tránsito y Seguridad Vial en el

territorio nacional" [48] por intermedio de la Dirección de Tecnologías de la Información requiere realizar un Análisis de Riesgos de una posible migración de su actual Sistema Recaudo hacia la Nube. Requerimiento tecnológico que será atendido mediante la aplicación del "Modelo de Gestión de Riesgos" propuesto en el presente trabajo de titulación.

Cabe indicar que el alcance del presente trabajo solo contempla los procesos de Gestión de Riesgos esquematizado en la Figura 2.2.1.1, más no, la implementación del modelo de despliegue o servicio de nube analizado. Requerimiento que puede ser atendido mediante la aplicación de trabajos académicos investigativos existentes como la "Guía Para el Análisis de Factibilidad en la Implantación de Tecnologías de Cloud Computing en Empresas del Ecuador" [58] disponible en la Biblioteca Virtual de la Escuela Politécnica Nacional.

3.2.1 FASE I: GOBIERNO DE NUBE

El Gobierno de Nube, según el modelo propuesto consta de los siguientes procesos, esquematizados en la Figura 3.2.1.1, mismo que permitirán asegurar que los riesgos relacionados con la Computación en la Nube no exceden ni el apetito ni la toleración de riesgo y que su impacto en el valor para la Agencia Nacional de Tránsito sean identificados, entendidos, articulados, gestionados y comunicados, para que en el peor de los casos, un potencial fallo en el cumplimiento sean reducidos al mínimo.

Figura 3.2.1.1 Procesos de la Fase 1 – Gobierno de Nube

3.2.1.1 Necesidad de Nube

La Dirección Ejecutiva de la Agencia Nacional de Tránsito, como parte del proceso de Innovación Tecnológica del Transporte, ha visto la posibilidad de migrar su actual "Sistema Integrado de Recaudación del Transporte Público Urbano de los cantones de Santa Elena, la Libertad y Salinas" hacia la Nube, para lo cual requiere de la Dirección de Tecnologías de la Información y Comunicación, el desarrollo de una metodología estructurada, consistente y contínua de Gestión de Riesgos de Servicios en la Nube, adaptada a la realidad nacional, para que sea implementada a través de toda la organización – directorio, jefes de área y resto de personal – a fin de que los resultados que se obtenga de dicha metodología sean puestos a consideración del directorio para su aprobación o veto definitivo.

3.2.1.2 Objetivos Organizacionales y de Nube

En general, toda organización como objetivo de gobierno existe para crear valor para sus partes interesadas. Es decir, obtener beneficios a un coste óptimo de recursos mientras se optimiza el riesgo, que en el caso de la Agencia Nacional de Tránsito por ser una entidad gubernamental se traducen en servicios al ciudadano. De acuerdo al marco de trabajo COBIT5, en la Tabla 3.2.1.1, se puede establecer los siguientes objetivos organizacionales alineados con la gestión de riesgos de servicios en la Nube como apoyo a los objetivos estratégicos y requerimientos de las partes interesadas.

Dimensión CMI	**Objetivos/metas Organizacionales**		**Relación con los objetivos de gobierno**		
			Realización de Beneficios	Optimización de Riesgos	Optimización de Recurso
Financiera	02	Cartera de productos y servicios competitivos	P	P	P
	03	Riesgos de negocio gestionados (salvaguarda de activos)		P	S
	04	Cumplimiento de leyes y regulaciones externas		P	
Cliente	07	Continuidad y disponibilidad del servicio de negocio		P	
	09	Toma estratégica de Decisiones basada en Información	P	P	P
Interna	13	Programas gestionados de cambio en el negocio	P	P	P
	15	Cumplimiento con las políticas internas		P	

Aprendizaje y Crecimiento	16	Personas preparadas y motivadas		P	P

Tabla 3.2.1.1: Objetivos organizacionales relacionados con la Computación en la Nube según COBIT 5

Objetivos organizacionales de la Tabla 3.2.1.1, desarrollados utilizando las dimensiones del cuadro de mando integral (CMI) y que tiene una relación Principal (P) con la Optimización de Riesgos, uno de los principales objetivos del Gobierno de Nube, según la metodología propuesta. Sin embargo, como es de esperarse el logro de los objetivos organizacionales requiere de objetivos relacionados con la Información y con la Tecnología (TI), que de acuerdo a COBIT5, se identifican cuatro objetivos de TI para asegurar la Optimización del Riesgo, principal meta del Gobierno de Nube, como se evidencia en la Tabla 3.2.1.2:

Objetivo GOBIERNO DE NUBE (COBIT5)			**DIMENSIÓN DEL CMI TI**	**OBJETIVOS RELACIONADOS CON TI.**	
ÁREA	**DOMINIO**	**PROCESO**			
GOBIERNO	**Evaluar, Orientar y Monitorear**	**EDM03: OPTIMIZACIÓN DEL RIESGO**	Financiera	04	Riesgos de negocio relacionados con la Nube
				06	Transparencia de los costes, beneficios y riesgos de Nube
			Internas	10	Seguridad de la información, infraestructura, plataforma y aplicaciones
				15	Cumplimiento de las políticas internas por parte de la Nube

Tabla 3.2.1.2: Objetivos de TI relacionados con la Computación en la Nube según COBIT 5

Objetivos organizacionales y objetivos de TI, mapeados en la Tabla 3.2.1.3, a fin de establecer como son soportados entre sí y descartar aquellos objetivos cuya relación no es importante (P) o fuerte (S) en el cumplimiento de los objetivos estratégicos planteados por la Agencia Nacional de Tránsito.

	OBJETIVO CORPORATIVO							
	02 Cartera de productos y servicios competitivos	**03 Riesgos de negocio gestionados (salvaguarda de activos)**	**04 Cumplimiento de leyes y regulaciones externas**	**07 Continuidad y disponibilidad del servicio de negocio**	**09 Toma estratégica de Decisiones basada en Información**	**13 Programas gestionados de cambio en el negocio**	**15 Cumplimiento con las políticas**	**16 Personas preparadas y motivadas**

Objetivo Relativo a TI		FIN			CLI		INT		APR
FIN	**04 Riesgos de negocio relacionados con la Nube**		P	S	P		S	S	S
	06 Transparencia de los costes, beneficios y riesgos de Nube		S			S			
INT	**10 Seguridad de la información, infraestructura, plataforma y aplicaciones**		P	P	P			P	
	15 Cumplimiento de las políticas internas por parte de la Nube		S	S				P	

Tabla 3.2.1.3: Mapeo Objetivos Organizacionales y Objetivos de TI

Como resultado del mapeo de la Tabla 3.2.1.3, donde INT – Interno, FIN – Financieros, CLI – Cliente, APR – Aprendizaje y Monitoreo; se establece como prioritarios las siguientes metas u objetivos organizacionales y de TI, para el Modelo de Gestión de Riesgos" propuesto:

- Objetivos o metas organizacionales:
    - 03 Riesgos de negocio gestionados (salvaguarda de activos)
    - 04 Cumplimiento de leyes y regulaciones externas a la organización
    - 07 Continuidad y disponibilidad del servicio de negocio
    - 15 Cumplimiento con las políticas internas de la organización
- Objetivos o metas de TI
    - 04 Riesgos de negocio relacionados con la Nube
    - 10 Seguridad de la información, infraestructura, plataforma y aplicaciones

3.2.1.3 Estructura Organizacional

Los objetivos y/o metas organizativas y de TI, identificadas en el apartado anterior necesitan de estructuras organizativas y roles para operar, ya que constituyen uno de los puntos clave para garantizar la seguridad de los activos de información contra acceso, divulgación, modificación, destrucción e interferencia no autorizados [45], más aún, para ambientes de Nube, donde las responsabilidades del cliente y del proveedor deben estar claramente establecidas, como el propuesto en el anexo 3.

En la Tabla 3.2.1.4, se presenta la estructura organizacional que se empleará en el "Modelo de Gestión de Riesgos de Infraestructura como Servicios (IaaS)", resultado del mapeo entre el Orgánico Funcional por Procesos de la Agencia Nacional de Tránsito, el marco de trabajo COBIT5 y la norma técnica NTE INEN-ISO/IEC 27000, en la que se identifica claramente a los responsables, a quienes deben rendir cuentas, a los consultados y a los informados; cada uno organizado por roles organizacionales y de TI.

FASES MODELOS DE GESTIÓN DE RIESGOS IaaS	ROLES Y RESPONSABILIDADES									
	ORGANIZACIONAL								TI	
	Consejo Directivo o Directorio	Director Ejecutivo (CEO)	Dirección de Planificación /Contratación	Oficial de Seguridad (CSO/CRO)	Responsable de la Seguridad de la Información (CISO)	Comité de Gestión de Riesgos (CGR)	Dirección de Asesoría Jurídica (Compliance)	Auditoría Interna	Director de Tecnologías de la Información (CIO)	Director Técnico
GOBIERNO DE NUBE	A	R	I	R	RCI	I	C	C	R	C
CONSIDERACIONES NUBE	C	A	I	RC	RC	I	C	C	R	R
GESTIÓN DE RIESGOS		I	RC	RA	RC	I	RC	RC	RA	RC

Tabla 3.2.1.4: Mapeo Estructuras Organizativas ANT, ISO27000 y COBIT5 – Matriz RACI

De acuerdo a la Tabla 3.2.1.4, los niveles de implicancia en la estructura organizacional propuestas son [59]:

- R(esponsable) — Quién está haciendo la tarea? Hace referencia a los roles que se encargan de la actividad principal para completar la actividad y producir la salida esperada.

- A(responsable de que se haga) — ¿Quién rinde cuentas sobre el éxito de la tarea? Asigna la responsabilidad de consecución de la tarea (donde termina la responsabilidad). Tenga en cuenta que el rol mencionado es el nivel más bajo apropiado para rendir cuentas; hay por supuesto, más altos niveles de rendición de cuentas también. Para activar la potenciación de la organización, la responsabilidad de rendir cuentas se descompone con la mayor granularidad posible. La rendición de cuentas no indica que el rol no tenga actividades operativas; es probable que el

rol se involucre en la tarea. Como principio, la rendición de cuentas no puede ser compartida.

- C(onsultado) — ¿Quién proporciona entradas? Estos roles que proporcionan entradas son clave. Tenga en cuenta que corresponde a los roles de responsable y de rendir cuentas, obtener información de otras unidades o, también de, interesados externos. En cualquier caso, las entradas de estos roles enumerados deben ser consideradas y, si se requiere, tomar las medidas necesarias para que se escalen, incluyendo la información del propietario del proceso y/o del Comité de Dirección.

- I(nformado) — ¿Quién recibe la información? Estos son los roles que son informados de los logros y/o entregables de las tareas. Por supuesto, el rol del 'responsable de hacer' debe recibir siempre información apropiada para supervisar la tarea, al igual que los roles responsables del área de interés.

A continuación se describe los roles, funciones y responsabilidades de la estructura organizacional propuesta, necesarias para ir a la Nube:

- Consejo Directivo o Directorio.- Es el grupo de más alto nivel ejecutivo y no ejecutivo de la Agencia Nacional de Tránsito, quienes son responsables del gobierno corporativo y tienen control global sobre los recursos. Entre su funciones se tiene:

    - Supervisa el impacto del riesgo corporativo sobre los objetivos corporativos y toma decisiones sobre el riesgo para proteger el valor de los accionistas a un óptimo costo de los recursos.

    - Establece el tono directivo respecto a la gestión y la concientización del riesgo.

- CEO (Chief Executive Officer) o Director Ejecutivo.- Es la máxima autoridad de la Agencia Nacional de Tránsito a cargo de la Dirección Ejecutiva, quién debe ofrecer apoyo ejecutivo y colaborar en las decisiones de gestión de riesgos, a fin de asegurar la implementación y funcionamiento del Modelo de Gestión de Riesgos de Infraestructura como Servicios (Iaas) de Cloud Computing en la Agencia Nacional de Tránsito, asignando para ello los recursos necesarios. Entre sus funciones se incluyen:

- Conformar el Comité de Gestión de Riesgos (CGR) y designar sus integrantes
- Supervisar y velar porque la estrategia y objetivos organizacionales se cumplan, además de establecer los principios y pilares básicos para la gestión de riesgos.
- Establecimiento de relación con el CIO, debido a que las estrategias de la organización y la gestión de riesgos están estrechamente ligadas con las tecnologías de la información.

- Comité de Gestión de Riesgos (CGR).- Grupo de ejecutivos de la Agencia Nacional de Tránsito designados por el Directorio para que se involucren e informen de las principales decisiones y aspectos relacionados con TI. Son responsables de la gestión del portafolio de inversiones habilitadas por TI, así como los servicios y activos de TI, asegurando la entrega de valor y la gestión de los riesgos. El comité estará dirigido por un miembro del consejo directivo (CISO) y no por el Director de TI (CIO). Entre sus responsabilidades se incluye:
  - Involucrar la participación y cooperación de los cargos directivos de la institución en la gestión de riesgos
  - Proactividad en la gestión de los riesgos relacionados con el portafolio de las inversiones de TI.
  - Monitorear cambios significativos de los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
  - Acuerda y aprueba metodologías y procesos específicos para la gestión de riesgos, en base a las normas NTE INEN-ISO/IEC 27000.
  - Evalúa y coordina la implementación de controles específicos para la gestión de riesgos de servicios en la Nube.
- CSO (Chief Security Officer) u Oficial de Seguridad.- Es el responsable de la seguridad organizativa o corporativa. Con roles diferentes al CISO, el cual está más centrado en aspectos de seguridad de la información. Entre sus responsabilidades se incluyen:

- No pertenece al área de Tecnologías de la Información y reporta a la máxima autoridad de la institución.
- Define procedimientos para el manejo de incidentes de seguridad y para la administración de los medios de almacenamiento y respaldos.
- Define y documenta controles para la detección y prevención del acceso no autorizado, la protección contra software malicioso, garantiza la seguridad de los datos y los servicios conectados a las redes de la institución.
- Tiene una visión de negocio para comprender los riesgos que afronta la organización y cómo tratarlos.
- Entiende la misión y los objetivos organizacionales y asegura que todas las actividades son planificadas y ejecutadas para satisfacer dichos objetivos.
- Comprende las necesidades normativas, la gestión de la reputación de la organización y proveedores, y las expectativas de los usuarios.
- Establece planes de continuidad de negocio y recuperación de desastres en el ámbito de las tecnologías de la información.
- Está al tanto de los cambios normativos, debiendo informarse de las consecuencias para las actividades de la organización y proponiendo las medidas oportunas para adecuarse al nuevo marco normativo.

- CISO (Chief Information Security Officer) o Responsable de la Seguridad de la Información.- Es un rol desempeñado a nivel directivo por un consultor en riesgos de seguridad y su función principal es la de alinear la seguridad de la información con los objetivos de negocio y coordinar la respuesta a incidentes, de esta forma se garantiza la seguridad de la información de la Agencia Nacional de Tránsito en todas sus formas. Entre sus responsabilidades se incluyen:
  - Evalúa el posible impacto operativo a nivel de seguridad de los cambios previstos a sistemas y equipamiento, y verifica su correcta implementación, asignando responsabilidades.
  - Monitorea las necesidades de capacidad de los sistemas en operación y proyecta las futuras demandas de capacidad para soportar potenciales amenazas a la seguridad de la información que procesan.

- Asegura el registro de las actividades realizadas por el personal operativo de seguridad de la información, para su posterior revisión.
- Gestiona los incidentes de seguridad de la información de acuerdo a los procedimientos establecidos.
- Genera e implanta políticas de seguridad de la información.
- Garantiza la seguridad y privacidad de los datos.
- Supervisa la administración del control de acceso a la información.
- Supervisa el cumplimiento normativo de la seguridad de la información.
- Supervisa la arquitectura de seguridad de la información de la organización.
- Designa al Responsable Técnico (CTO) de la Dirección de Tecnologías de la Información en coordinación de su director.

- Dirección de Planificación/Contratación.- Desarrolla e implementa estrategias, planes, programas, proyectos, investigaciones y el sistema institucional que contribuyan al fortalecimiento de la gestión institucional y del sistema integrado de información del sector. Entre sus responsabilidades se incluyen:
  - Disponer y verificar las acciones de diseño e implementación y mantenimiento del sistema integrado de información que permita una efectiva planificación y toma oportuna de decisiones.
  - Diseñar e implementar herramientas, medios y tecnología de punta que permitan optimizar la gestión institucional y la atención al usuario, sobre la base del sistema integrado de información.
  - Desarrollar e implementar estándares e indicadores de gestión administrativa y presupuestaria de los proyectos inherentes a la ANT.
  - Coordinar la elaboración de informes estadísticos sectoriales y consolidar la información relacionada con indicadores de gestión respecto al transporte terrestre, tránsito y seguridad vial.
- Dirección de Asesoría Jurídica.- Supervisa e informa sobre el estado de cumplimiento de la Agencia Nacional de Tránsito respecto a las leyes y normas

pertinentes. Asegura que los requerimientos de cumplimiento sean comprendidos, comunicados, respetados y que se corrijan las áreas de incumplimiento, a todo nivel organizacional. Asegura la alineación con el enfoque global del ERM (si existe), confirma que los objetivos pertinentes y la gestión del riesgo se cumplan, que los temas sean considerados y que los beneficios sean alcanzados. Además, se encarga de:

- Absolver consultas de las unidades Institucionales a nivel nacional, en lo relacionado con aspectos jurídicos en general, para la toma oportuna y legal de decisiones
- Ejercer la representación legal, judicial y extrajudicial de la ANT.
- Coordinar, controlar y aprobar la elaboración de anteproyectos de ley, acuerdos y reglamentos.
- Coordinar la aplicación de normas y directrices legales provenientes de la Presidencia de la República, la Secretaría de la Administración Pública y organismos de control.
- Proporcionar asesoría jurídica a las autoridades y direcciones de la institución en materias que se hallen dentro de la competencia jurídica y legal.
- Dirigir la elaboración de los proyectos que se requieran y toda la documentación necesaria.
- Responder y emitir los respectivos criterios jurídicos, ante consultas formuladas por las autoridades, funcionarios y servidores de la Institución

- Auditoría Interna.- Realiza el control posterior a las operaciones administrativas y financieras, y el asesoramiento concurrente de conformidad a lo dispuesto a la ley de Contraloría, a fin de asegurar la utilización eficiente y eficaz de los recursos y el mejoramiento de sus procesos institucionales. Definirá y ejecutará un plan de auditoría basado en las consideraciones de riesgo del negocio. Debe garantizar su independencia de manera absoluta cuando desempeña sus funciones de auditoría, pero, dentro de estos límites, puede dar consejos. El ámbito de control es toda la organización, pero reporta directamente al Consejo Directivo o Directorio de la ANT. Entre sus responsabilidades se incluyen:

- Realizar el seguimiento y aplicación de las recomendaciones impartidas por los organismos de control.
- Dirigir las actividades de auditoría de los sistemas informáticos de la Institución.
- Planificar y supervisar las actividades relativas a exámenes especiales de auditoría, a pedido de las autoridades.
- Asesorar a las autoridades y a los funcionarios con sujeción a las leyes y normas de auditoría interna, en el análisis, desarrollo, implantación y mantenimiento de los sistemas y procesos Institucionales, a través de una participación activa y oportuna en el área de su competencia, y en función del mejoramiento contínuo del sistema de control interno de la entidad.
- Evaluar el cumplimiento de las recomendaciones constantes en los informes de auditoría interna y externa para determinar la continuidad de las acciones correctivas aprobadas por la máxima Autoridad.

- CIO (Chief Information Officer) o Director de Tecnologías de la Información.- Es el responsable de que las estrategias de la organización estén alineadas con la tecnología de la información para lograr los objetivos planificados. Reporta directamente al CEO. Además, se encarga de:
  - Mejorar los procesos de tecnologías de la información de la organización.
  - Gestionar el riesgo y la continuidad de negocio.
  - Controlar el coste en infraestructura de tecnologías de la información.
  - Alinear el gobierno de tecnologías de la información a los requerimientos tecnológicos, y
  - Establecer mejoras e innovaciones de soluciones y productos.
- CTO (Chief Technology Officer) o Director Técnico.- Se entremezclan con las funciones del CIO pero más técnico, siendo su responsabilidad la gestión del día a día de las tecnologías de la información.

Estructura organizacional, que se esquematiza en la Figura 3.2.1.2:

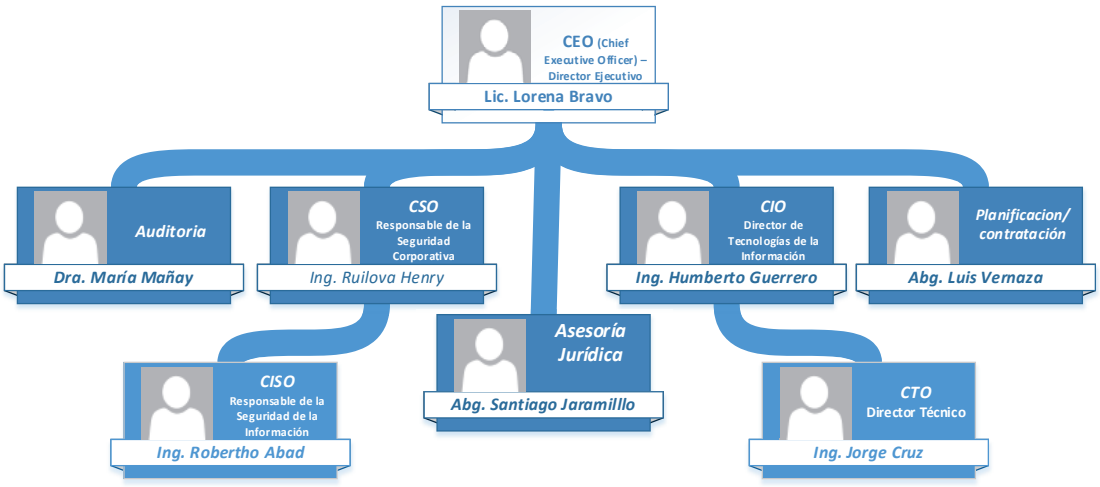

Figura 3.2.1.2 Roles, Funciones y Responsabilidades Gestión de Riesgos IaaS

3.2.2 FASE II: CONSIDERACIONES HACIA LA NUBE

Considerando que en el mercado ecuatoriano no existe metodología alguna que guie a la Agencia Nacional de Tránsito en su etapa inicial de gestión de riesgos de servicios de Nube, el modelo propuesto plantea para esta fase un conjunto de consideraciones de camino a la Nube, organizados en cuatro pasos esquematizados en la Figura 3.2.2.1, como resultado del análisis de iniciativas, estudios, mejores prácticas, normas, controles y métricas existente en la materia.

Figura 3.2.2.1 Consideraciones hacia la Computación a la Nube

3.2.2.1 Paso 1: Preparación del Medio Interno o Procesos del Negocio

Está claro que las iniciativas de la Computación en la Nube transforman el modelo de negocio tradicional al establecer un entorno de TI flexible y adaptable que satisfaga rápidamente las necesidades cambiantes de los procesos Gobernantes y

Agregadores de Valor, siendo responsabilidad de la Dirección de Tecnologías de la Información y Comunicación, en su calidad de proceso de apoyo a la gestión y consecución de objetivos y metas de la Agencia Nacional de Tránsito, desarrollar estrategias de preparación de camino a la Nube, como el que se propone a continuación.

3.2.2.1.1 Identificar lo que se va a mover a la Nube

No siempre una aplicación, plataforma o infraestructura de la que todos creen que podría ser idónea para ir a la nube lo es. Es necesario construir un caso de negocios que lo justifique, que para el caso particular de la Agencia Nacional de Tránsito lo constituye la CONTINGENCIA del Sistema Central del "Sistema Integrado de Recaudación del transporte público urbano de los cantones de Salinas, Libertad y Santa Elena – Recaudo", que entre otras cosas busca:

- Garantizar la seguridad y eficiencia en la operación de recaudación tarifaria.
- Promover una mejor calidad en el servicio de transporte público concesionado.
- *Garantizar la disponibilidad permanente del servicio de recaudación de transporte.*
- Establecer canales eficientes de distribución o expendio del medio de acceso.
- Evitar el desvío de recursos en todas las unidades destinadas a otorgar el servicio.
- Reducir el tiempo de embarque a las unidades, eliminando la necesidad de uso de efectivo.
- Permitir la interoperabilidad con otros sistemas de transporte.
- Permitir la implementación de políticas tarifarias, acorde a lo autorizado por el organismo competente.
- Establecer una mejor gestión de operación de rutas y unidades, al generar información que permita una mejor gestión del servicio por parte de las autoridades.

Al momento el Sistema Integrado de Recaudación se encuentra operando según esquema de la Figura 3.2.2.2, en 250 unidades de transporte urbano correspondiente a las nueve operadoras de Transporte Urbano de las ciudades de Santa Elena, Salinas y Libertad, al servicio de 110.000 habitantes pertenecientes a

la Población Económicamente Activa (PEA) de la Provincia de Santa Elena según el último censo de población y vivienda [60].

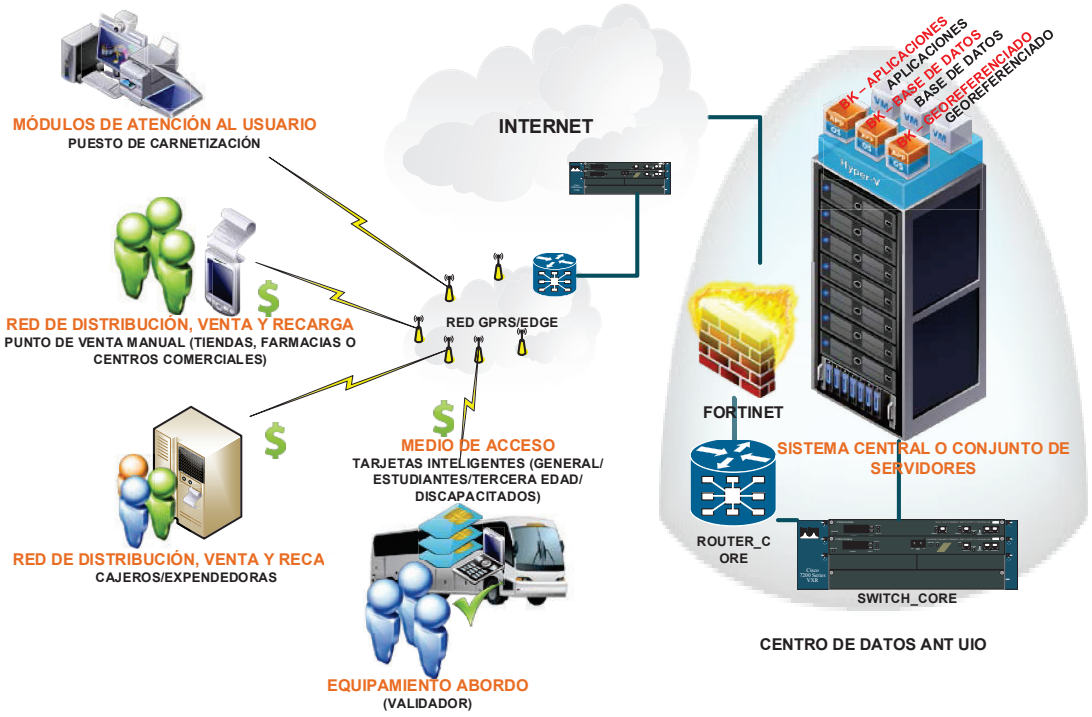

Figura 3.2.2.2 Esquema lógico Sistema Recaudo

De la Figura 3.2.2.2 se identifica los siguientes sistemas y componentes que conforman el Sistema de Recaudación, cuya arquitectura se resumen en la Figura 3.2.2.3:

- Equipamiento abordo en unidades de transporte:
    - Validador de tarjeta para cobro de la tarifa a bordo
    - Equipos de conteo de pasajeros (barras de conteo, torniquete de 3 brazos electromecánico o su equivalente)
    - Sistema de identificación de operador de la unidad, rutas, parámetros por aplicar a la unidad.
    - Alertas sonoras del uso de las tarjetas.
- Red de distribución, venta y recarga de las tarjetas

  - Máquinas o cajeros de recarga automáticas de tarjetas de transporte
  - Puntos de venta manual: tiendas, farmacias o centros comerciales.
- Medios de Acceso – Tarjetas inteligentes sin contacto
  - General
  - Estudiante
  - Tercera Edad
  - Discapacitados
- Módulos de atención de los usuarios
  - Equipos de asistencia al usuario: credencialización, reposición de tarjetas, consulta de saldos, reposición de saldos
  - Equipos para personalización y habilitación de tarjetas.
- Sistema central o conjunto de Servidores, para:
  - Almacenar en base de datos las transacciones del sistema
  - El monitoreo / control de las unidades
  - Generación de informes
  - Medición de los terminales
  - Gestión de la seguridad del sistema: Autenticación, encriptación, perfiles de usuarios, definición de derechos de acceso.
  - Gestionar parámetros de configuración Administrativos y Operativos del Sistema.
  - Gestionar la cámara de compensación para procesar los informes para determinar los pagos a las distintas operadoras (en caso de existir).

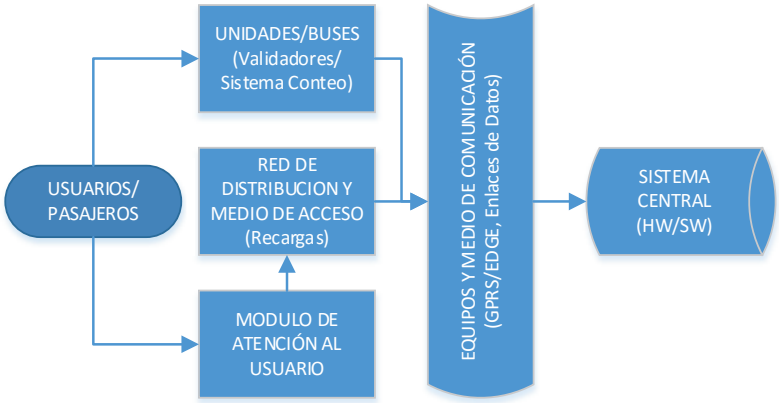

Figura 3.2.2.3 Arquitectura Sistema Recaudo.

De acuerdo a la Figura 3.2.2.3, el Sistema Central es la parte medular del Sistema Integrado de Recaudación al que convergen todos sus componentes constituyéndose en uno de sus puntos de fallo, que debe ser mitigado mediante su implementación en un sitio alterno, a fin de garantizar su disponibilidad y cumplir con los objetivos inicialmente planteados.

En la Tabla 3.2.2.1, se detalla el hardware y/o software requerido para el correcto funcionamiento del Sistema de Contingencia del Sistema Central del Sistema Recaudo.

Can.	MARCA	MODELO	Descripción	ESPECIFICACIONES TÉCNICAS
1	Beacoud	Rack 36UR		Rack cerrado de 36UR
1	HP	ProLiant DL320e Gen8	Servidor de Aplicaciones	1 CPU Intel Xeon E3-1220v2 4 Core 3.10GHz Memoria Cache 8MB 8GB RAM Total (2 x 4GB) PC3-12800 DDR3 1600MHz 4 Discos Duros 1TB 6G 7.2KRPM HPL SATA LFF (3.5in)
2	HP	ProLiant DL320e Gen8	Servidor de Base de Datos	1 CPU Intel Xeon E3-1220v2 4 Core 3.10GHz Memoria Cache 8MB 8GB RAM Total (2 x 4GB) PC3-12800 DDR3 1600MHz 4 Discos Duros 1TB 6G 7.2KRPM HPL SATA LFF (3.5in)
2	HP	ProLiant DL320e Gen8	Servidor Georeferenciado	1 CPU Intel Xeon E3-1220v2 4 Core 3.10GHz Memoria Cache 8MB 8GB RAM Total (2 x 4GB) PC3-12800 DDR3 1600MHz 4 Discos Duros 1TB 6G 7.2KRPM HPL SATA LFF (3.5in)
2	MS	Windows Server	Sistema Operativo	Server 2012 R2 Datacenter Licencia, incluye dos instancias virtuales. (2) $882,00
2	MS	Windows Server	Sistema Operativo	Server 2012R2 OLP NL Gov 2Proc (2) $900,00
2	MS	Windows Server	Sistema Operativo	MS WinSvrCAL 2012 OLP NL Gov UsrCAL (2) $38,80
2	MS	SQL Server	Motor BDD	MS SQL Server Standard Edition License y Software (2)
2	MS	SQL Server	Motor BDD	Microsoft SQL Server 2012 - License - 1 user (2) CAL $300,00

Tabla 3.2.2.1: Hardware y software requerido para Sistema Recaudo

Al Hardware y Software de la Tabla 3.2.2.1, se debe incorporar los requerimientos ambientales, eléctricos y de seguridad con el que cuenta el Centro de Datos – Tabla 3.1.5.5 – y los equipos de comunicación (router y switch), sistema de seguridad perimetral, sistema de respaldo y el servicio de enlace de datos e internet; sistemas y servicios requeridos para garantizar el acceso, disponibilidad, seguridad e integridad del Sistema Integrado de Recaudación, mismos que se resumen en la Tabla 3.2.2.2.

No.	DESCRIPCIÓN	CANT
1	Equipos de Seguridad Informática “Fortigate 3040B”	2
2	Equipo de Análisis y Almacenamiento de Log’s “FortiAnalyzer 2000B”	1
3	Router Core Cisco 4400 Series	2
4	Switches de Core Cisco Catalyst 4507R+E	2
5	Switch de Distribución Cisco 4500X Series	2
6	Enlace de Datos Principal 40Mb F.O. ANT - Data Center CNT	1
7	Enlace de Datos Backup 20Mb F.O. ANT - Data Center CNT	1
8	Enlace de Internet Principal 40Mb F.O. ANT	1
9	Enlace de Internet Backup 20Mb F.O. ANT	1
10	Herramienta de Backup Corporativa TSM TIVOLI (10TB)	1

Tabla 3.2.2.2: Equipos de comunicación, seguridad perimetral, respaldos y enlaces de datos e internet.

Por lo expuesto y a fin de eliminar los puntos únicos de fallos que atentan contra la disponibilidad del “Sistema Integrado de Recaudación del Transporte Público Urbano de los cantones de Santa Elena, la Libertad y Salinas”, el Directorio de la Agencia Nacional de Tránsito ha identificado la necesidad de migrar la Contingencia del “Sistema Central Recaudo” hacia la Nube, para garantizar la movilidad y libertad del transporte urbano de los ciudadanos de los cantones de la provincia de Santa Elena bajo los principios de seguridad, eficiencia, responsabilidad, universalidad, accesibilidad, continuidad y calidad, contribuyendo al desarrollo socio-económico del país.

3.2.2.1.2 Validar que la infraestructura se complementa y esté listo para moverse a la Nube

Al momento la Agencia Nacional de Tránsito cuenta con un 80% de su infraestructura de servidores – Tabla 3.1.5.3 y Tabla 3.1.5.12 – virtualizados tanto a nivel de Software (VMware) como de Hardware (PowerVM), ver Figura 3.2.2.4, el

20% restante corresponde a servidores ejecutando aplicaciones heredadas o propietarias.

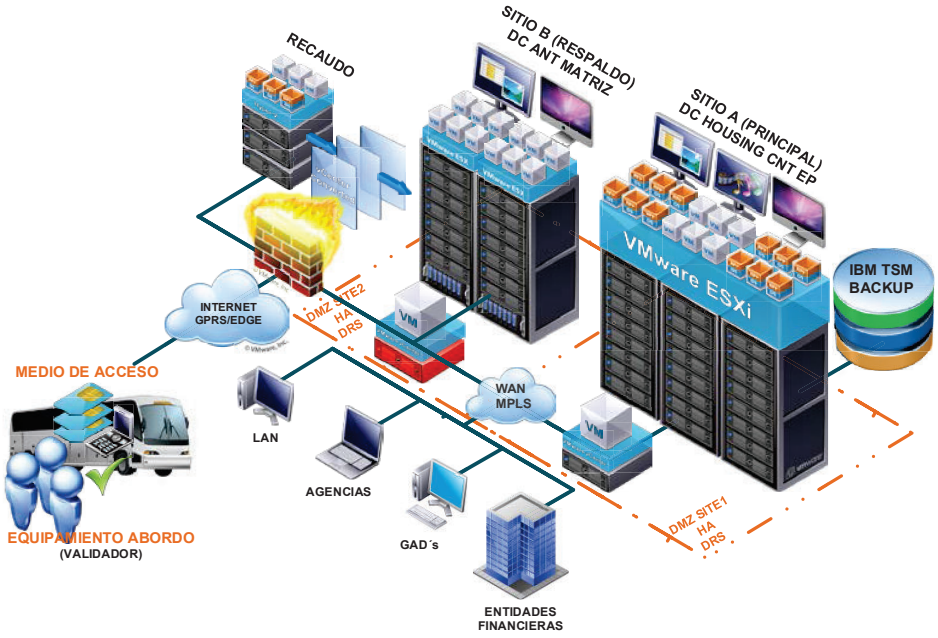

Figura 3.2.2.4 Ambiente de virtualización ANT – Recaudo.

Ambiente Virtualizado por Software, de la Figura 3.2.2.4, operando en alta disponibilidad (HA) y con cargas de trabajo bien distribuidas (DRS) entre ambos centros de datos, características únicas de VMware [61], que le permite a la Dirección de Tecnologías de la Información aprovechar los siguientes beneficios esquematizados en la Figura 3.2.2.5:

- Mejorar los niveles de servicio asegurándose de que las máquinas virtuales dispongan de los recursos apropiados.
- Implementar más capacidad en un clúster o Centro de Datos sin interrumpir el servicio.
- Migrar automáticamente las máquinas virtuales durante las tareas de mantenimiento sin interrumpir el servicio.
- Supervisar y gestionar más cantidad de infraestructura por cada administrador del sistema.

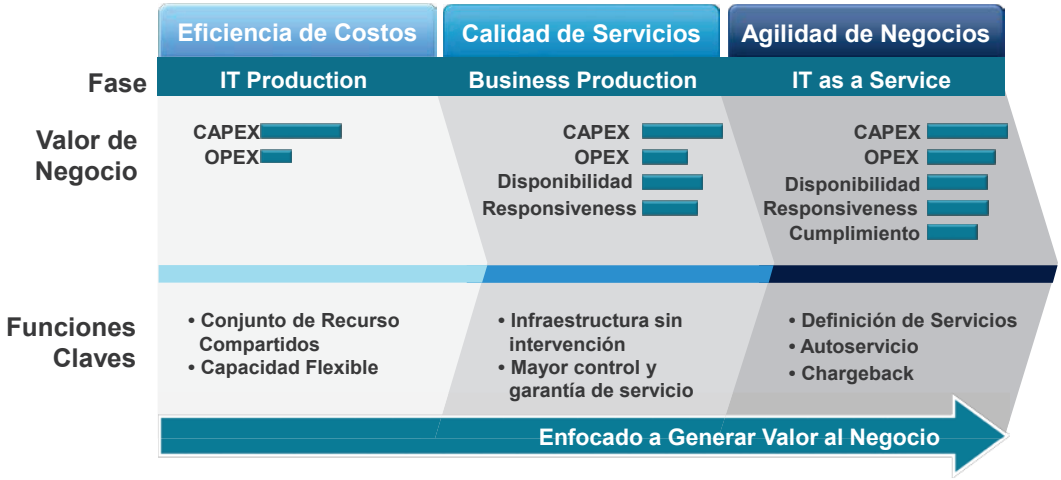

Figura 3.2.2.5 Beneficios del licenciamiento VMware v Sphere Enterprise Plus [61].

Parte de este ambiente virtualizado lo integra los servidores de aplicación, base de datos y georeferenciado del Sistema Integrado de Recaudación, pero que debido las especificaciones técnicas contenidos en los pliegos se encuentran operando bajo hipervisor Hyper-V de Microsoft Server 2012. Hipervisores VMware ESXi e Hyper V, no compatibles entre sí, pero que cuentan con herramientas adicionales como VMware vCenter Converter [61] o Microsoft Virtual Machine Converter (MVMC) [62] respectivamente, como solución alternativa para la consolidación de cargas de trabajo y/o servicios bajo VMware vSphere, que de acuerdo al esquema de la Figura 3.2.2.6, ofrece a aquellos usuarios operando bajo centro de datos definidos por software un camino sencillo hacia la nube.

Por lo expuesto se evidencia que la infraestructura de virtualización del Sistema Integrado de Recaudación si se complementa tanto con la infraestructura de TI que se maneja en la Agencia Nacional de Tránsito como el de la Computación en la Nube, pero dichos costos deberán ser asumidos por la institución, en el caso de una posible adopción de la computación en la nube de la Contingencia del Sistema Central Recaudo.

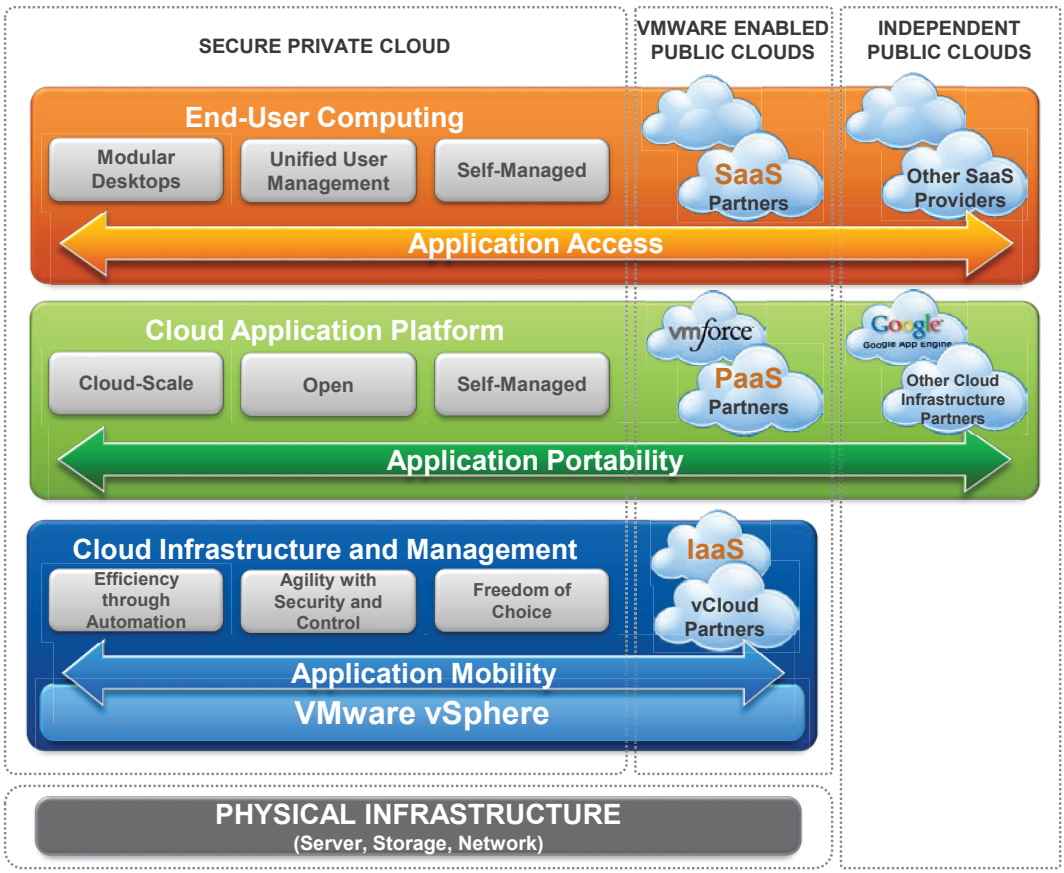

Figura 3.2.2.6 A un paso de la Nube con VMware vSphere [61].

3.2.2.1.3 Marco Legal Local Aplicable

Pese a que el estado ecuatoriano no cuenta con un marco jurídico riguroso que ampare normativamente el desarrollo del mercado de la Computación en la Nube, la Agencia Nacional de Tránsito en su calidad de entidad Gubernamental y en aplicación del acuerdo ministerial 166, al momento puede contratar, acceder o usar servicios de Computación en la Nube, siempre y cuando, el Proveedor seleccionado se someta a la Constitución y Leyes Ecuatorianas listadas en la Tabla 2.2.3.1, es decir, que su centro de datos, redes, equipos, software base y de gestión, y cualquier elemento tecnológico necesario para el procesamiento de la información se encuentre en el territorio nacional.

Adicionalmente, considerando el vacío legal de la Agencia Nacional de Tránsito en el ámbito de Computación en la Nube, previamente analizados en los numerales 3.1.3 y 3.1.5.3, la Constitución de la República del Ecuador, la Ley de comercio electrónico, firmas electrónicas y mensajes de datos y las Normas Técnicas

Ecuatorianas NTE INEN-ISO/IEC 27000, se constituyen en los instrumentos jurídicos aplicables en su afán de garantizar los tres pilares fundamentales de la seguridad de la información, a los cuales se pueden incorporar iniciativas metodológicas de organismos internacionales, como la ISO, la CSA, el NIST y la DMTF, adaptados al entorno nacional y organizacional.

3.2.2.1.4 Contrato y Acuerdos de Nivel de Servicios (SLA)

Dada la heterogeneidad de los servicios de Nube, los contratos y acuerdos de nivel de servicios se constituyen en el medio mediante el cual las entidades gubernamentales garantizan que sus obligaciones respecto a la soberanía y protección a la seguridad de la información se extiendan al proveedor de Nube y a sus terceros. Sin embargo, considerando que en el ámbito de Contratación Pública Ecuatoriana aún no se dispone de procedimientos específicos para la contratación de servicios de Nube, se deberá observar la amplia normativa existen a nivel internacional (EEUU y UE), a fin de que complementen a las leyes y reglamentos nacionales y permita al personal de la Agencia Nacional de Tránsito identificar los aspectos esenciales del contrato, que deben tomarse en consideración tanto desde el punto de vista técnico como jurídico para garantizar la integridad, seguridad, confidencialidad y cumplimiento de la normativa relativa a la protección de datos.

En cualquier caso, la posición jurídica de la Agencia Nacional de Tránsito durante la vigencia del contrato de servicios de Nube debe ser la de responsable del tratamiento, pues a ella le corresponde la decisión sobre la finalidad, el contenido y el uso del tratamiento, así como la decisión sobre optar por el modelo de servicio y de despliegue en la Nube.

En el ANEXO 4, se propone un conjunto de cláusulas que podrían ser empleadas y modificadas por las diferentes entidades de la Administración Publica Ecuatoriana al momento de realizar la negociación, renovación o finalización con un proveedor de Nube, mismas que contemplan temas de interés mutuo como:

- Borrado seguro de la información (no mantener copia de información proporcionada) , de ser el caso colaboración en la transferencia hacia otro proveedor

- Ubicación de la Información dada la flexibilidad que provee la nube con las implicancias regulatorias foráneas que implica esto, por lo tanto, no transferir información a otro país sin la previa autorización del cliente.
- Pérdida de información, cláusula con un límite de responsabilidad hacia el proveedor
- Seguridad de la información, proveedor certificado en estándares internacionales para la gestión de la seguridad de datos, sumado el cifrado de datos, VPN, etc.
- Disponibilidad de la información.
- Implementar cláusulas específicas en el contrato, para establecer el compromiso del proveedor a no violar la confidencialidad de los datos, ni hacer uso de ellos durante la relación contractual ni al verse finalizada.
- Incluir los representantes del departamento Legal y de Contratación en el establecimiento del contrato, para asegurarse de que el proveedor cumpla con las obligaciones de normas y estándares.
- Establecer una cláusula en el contrato, para especificar el derecho del cliente a auditar al proveedor, especialmente cuando la organización tiene que cumplir algún requisito normativo sobre el servicio que está corriendo sobre la Nube. La auditoría podría verse sustituida si el proveedor de servicio presenta ante sus clientes alguna certificación relacionada con sistemas de gestión de seguridad, como el caso de la Norma ISO 27000.
- Por último, los contratos de acuerdo de servicio (SLA), deben ser revisados y creados específicamente, detallando los controles, normativas, medidas de protección, plazos de recuperación del servicio.

3.2.2.1.5 Análisis Fortalezas Oportunidades Debilidades y Amenazas (FODA)

Una vez que se tiene claro lo que se desea mover a la nube y que ésta se complementa con la infraestructura interna de TI, es necesario realizar una síntesis de las fortalezas, oportunidades, debilidades y amenazas identificadas en el capítulo 1, como herramienta de apoyo tanto a nivel operativo y directivo de la Agencia Nacional de Tránsito en su análisis y valoración de cada modelo de

despliegue y de servicio de Nube, ya que contrasta tanto los aspectos internos de la administración pública (fortalezas y debilidades) como los factores externos y fuera de su control (oportunidades y amenazas). Análisis de fortalezas, oportunidades, debilidades y amenazas de camino a la Nube resumidas en la Tabla 3.2.2.3.

	FORTALEZAS	DEBILIDADES
ANÁLISIS INTERNO	Eliminación costos de inversión inicial y de mantenimiento en infraestructura tecnológica. Flexibilidad y escalabilidad en la gestión de la variabilidad de la demanda, pago por uso. Eliminación de duplicidades y redundancias. Principal beneficio orientado hacia la ciudadanía. Conceptos relativamente nuevos en la región y en el país, por lo que su expansión se debe realizar de forma controlada. Alta oferta de proveedores nacionales e internacionales, apegados a estándares y mejores prácticas del sector. Concentración y fortalecimiento en la gestión de la seguridad. Profesionalización y excelencia en su administración. Aplicaciones, plataforma o infraestructura estable y de alta disponibilidad. Reducción al mínimo los tiempos de inactividad.	Deslocalización de la información y pérdida de control. Problema de gobernanza en el proceso de transformación hacia servicios compartidos. Inexistencia de procedimientos específicos para la contratación de servicios de Nube. Falta de una cultura de Seguridad de la Información, en proveedores y clientes. Dependencia de los proveedores de servicios por centralización de recursos de TI. Falta de amortización de los recursos TI. Desconocimientos de Computación en la Nube, tanto de sus beneficios como de sus debilidades. Falta de consideraciones previas a la contratación y durante la prestación del servicio. Oficinas y dependencias administrativas sin cobertura de Fibra Óptica (Galápagos) lo que limitan el acceso/consumo de Nube Falta de control sobre la cadena de suministro. Ingresos vulnerables y pérdida de imagen organizacional por fallos de seguridad, disponibilidad y rendimiento.
	OPORTUNIDADES	**AMENAZAS**
ANÁLISIS EXTERNO	Lecciones aprendidas del sector privado. Predilección por proveedores nacionales dada la normativa legal vigente (Régimen Especial). Inversión gubernamental en proveedores nacionales (empresa pública). Incremento cobertura de Fibra Óptica en el territorio continental. Reducción del presupuesto General de Estado por emitente crisis económica. Permitir a entidades gubernamentales con presupuestos limitados estar a la vanguardia tecnológica, centrando todos sus esfuerzos hacia su Core Business. Facilidad y rapidez de integración con el resto de aplicaciones.	Objetivo atractivo para ataques con motivos políticos e impactos elevados. Ausencia de normativa legal local que regule la prestación de servicios en la Nube. Proveedores no certificados en estándares de Seguridad de la Información. Monopolio por parte de pocos proveedores que pueden brindar el servicio de Nube. La confiabilidad de los servicios depende de la salud tecnológica y financiera del proveedor. Dificultad para acceder a registros y/o datos de auditoria (Informática forense). Dificultad para transferir datos de vuelta al usuario o proveedor alternativo elegido, por adopción de formato propietario para almacenar datos. Deterioro del rendimiento por compartición de recursos o sobredimensionamiento de las capacidades del proveedor (Fallo de aislamiento). Mercado inmaduro y no posesionado a nivel gubernamental. Entidades gubernamentales con asignación presupuestaria para TI holgada, que genera reticencia en la adopción de nube por contar con Centro de Datos Propios e infraestructura tecnológica de punta. Costos elevados si se desea garantizar los tres pilares fundamentales de la seguridad de la información, sin contar la alta disponibilidad, replicación y recuperación de desastres. Disminución de la velocidad de acceso por implementación de sistemas o protocolos seguros o por mala configuración de los mismos.

Tabla 3.2.2.3: Análisis FODA Computación en la Nube.

Cabe indicar que el establecimiento de fortalezas, oportunidades, debilidades y amenazas dependerá del modelo de despliegue y del modelo de servicio escogido, por ejemplo:

- En el establecimiento de los acuerdos de nivel de servicio.
- Grado de tolerancia a ataques maliciosos.
- En el establecimiento de requisitos y perfiles de riesgo.
- Establecimiento de perfil de control de acceso y autenticación.

De la Tabla 3.2.2.3, se evidencia que los factores externos, ajenos y fuera del control de la Agencia Nacional de Tránsito son los que deberán ser considerados con mayor énfasis por parte del nivel directivo en su camino a la nube, ya que por ejemplo, en ausencia o incumplimiento de la normativa legal vigente por parte de los proveedores, incrementaría la resistencia del sector público por adoptar la computación en la nube, más aún, si sectores estratégicos como el transporte que por generar su propios ingresos (autogestión) siempre contaran con una holgada asignación presupuestaria destinada a innovación tecnológica propia, que garanticen las capacidades requerida para asegurar la calidad del servicio a la ciudadanía.

3.2.2.1.6 Calculado el Retorno de la Inversión (ROI)

De acuerdo al reporte técnico “Calculando el ROI de la nube” de ISACA [63], el cálculo del Retorno de la Inversión (ROI) para el caso de estudio no es procedente, ya que la Agencia Nacional de Tránsito en su calidad de entidad de ***regulación*** y ***control*** del transporte terrestre, lo que busca con la ejecución de este proyecto es garantizar, al menos por los próximos 3 años, los principios de ***seguridad***, ***eficiencia***, ***accesibilidad***, ***continuidad*** y ***calidad*** de transporte terrestre en la provincia de Santa Elena, fomentando el principio de gestión empresarial por parte de sus operadoras de transporte urbano a través del uso de las Tecnologías de la Información y Comunicación [48], beneficios nada económicos o tangibles que se ajusten a las fórmulas tradicionales de cálculo del ROI.

Particular que se corrobora con el contrato y los términos de referencia del “Sistema Integrado de Recaudación del Transporte Público Urbano de los cantones de Santa Elena, la Libertad y Salinas”, donde se estable que la repartición de los ingresos por concepto de la venta y/o recarga de Tarjetas Inteligentes se lo realiza solo para las unidades de transporte urbano pertenecientes a las operadoras originalmente contempladas en el proyecto, sin beneficio económico alguno para la ANT, más que el acceso al sistema como mecanismo de supervisión y/o fiscalización para:

- Verificar la debida implementación del sistema.
- Validar la aplicación de las políticas tarifarias.
- Velar por el cumplimiento de las condiciones operativas conforme al contrato y términos de referencia.

Bajo esta consideración, lo más factible es realizar un análisis costo beneficio, que permita evaluar a la Computación en la Nube frente a otra solución alternativa, como el propuesto en la Tabla 3.2.2.4, donde una propuesta económica de un proveedor local para la prestación del servicio de Infraestructura como Servicio (IaaS) es analizada frente a un re-potenciamiento de la infraestructura tecnológica de la Agencia Nacional de Tránsito, ambas con el objetivo de garantizar por los próximos 3 años la alta disponibilidad y/o contingencia del Sistema Central del “Sistema Integrado de Recaudación del Transporte Público Urbano de los cantones de Santa Elena, la Libertad y Salinas”.

	Solución IaaS	**Re-potenciamiento infraestructura Actual**
Proveedor	Local	ANT
Periodo (meses)	36	36
Costo ($USD) (3 años)	306230	52000
tiempo de entrega	72 horas. No incluye tiempo instalación enlaces	60 días
Disponibilidad del Servicio (SLA/OLA)	99,98%	99,98%
Velocidad de Procesamiento (CPU) (GHz)	2,9	2,6
Procesadores Virtuales (vCPU)	12	32
Memoria RAM (GB)	32	128
Velocidad de Escritura en Disco (RPM)	7200	10000
Almacenamiento	12TB	19TB
Hipervisor	Microsoft	VMware
Alta Disponibilidad (HA)	Costo Adicional	Si contempla

Cargas de Trabajo Distribuidas (RDS)	Costo Adicional	Si contempla
Disponibilidad Datos e Internet	99,6% (Sin redundancia)	99,98 (Con redundancia)
Respaldos/backups	Costo adicional	Si incluye
Ancho de Banda enlace de Datos (Mbps)	10	40
Ancho de Banda enlace de Internet (Mbps)	5	40
Disponibilidad del Firewall	99,6% (Sin redundancia)	99,98 (Con redundancia)
Firewall	Software Sopho	Hardware Fortinet
Soporte y mantenimiento	3 años 24x7: IaaS y Firewall	3años: Hardware 24x7 y Firewall 9x5
Servicios de Migración	No incluye	No incluye
Licenciamiento MS WinSvr2012R2 y SQL2014	Costo Adicional	Sin incluye
Cumplimiento normativo local (acuerdo 166)	SI	SI
Auditoria y/o Informática Forense	NO	SI
Retorno o cambio de proveedor	NO	SI
Fallo de Aislamiento	NO	SI
Norma de Seguridad de la Información	SI	SI

Tabla 3.2.2.4: Análisis Costo Beneficio IaaS vs Re-potenciamiento Sistema Recaudo.

Análisis costo beneficio de la Tabla 3.2.2.4, económicamente nada favorable para la Computación en la Nube bajo modalidad Infraestructura como Servicio Pública, ya que las amenazas previamente identificas, terminan por imponerse sobre los beneficios esperados de la Nube.

En especial en un mercado poco desarrollado, que debido a normativas legales son muy pocas las empresas ecuatorianas [58] con la capacidad de proveer servicios en la nube a nivel empresarial o gubernamental, lo que termina por monopolizar el mercado de computación en la nube con costos muy elevados e inaccesibles para la mayoría de entidades gubernamentales que cuentan con asignaciones presupuestarias limitadas.

Adicionalmente, en base al reporte “Calculando el ROI de la Nube: Desde la Perspectiva del Cliente”, es necesario establecer los siguientes costos ocultos que la Agencia Nacional de Tránsito debe considerar de forma anticipada a fin de que las expectativas esperadas de un bajo coste de inicio y un rápido retorno de la inversión, no se vean afectados:

- Costo de implementar y operar en contramedidas para mitigar el riesgo: Sistema criptográficos, sistema autenticación doble factor, alta disponibilidad y redundancia, sistema de backups

- Gastos inesperados involucrados en la migración inicial de los sistemas: Incompatibilidad formatos de exportación, ventana de mantenimiento y tiempo de caída del sistema, licenciamiento adicional, sistemas heredados incompatible con la nube.
- La pérdida de conocimiento de TI interno que ofrece una diferenciación competitiva
- Costos por quedar atado a un proveedor de nube específico o a un modelo de servicio propietario, que puede desacelerar la futura adopción de servicios basados en estándares abiertos
- Costo por retorno de los servicios de Nube hacia la infraestructura organizacional.

3.2.2.2 Paso 2: Selección del Modelo de Servicio de Nube

Toda vez que la Agencia Nacional de Transito tanto a nivel directivo como operativo ha identificado la necesidad, los objetivos, la estructura organizacional y las consideraciones necesarias para una posible implementación del sitio alterno o contingencia del Sistema Central del "Sistema Integrado de Recaudación del Transporte Público Urbano de los cantones de Santa Elena, la Libertad y Salinas en la Nube", ahora es necesario identificar el modelo de servicio que mejor se alínea con sus objetivos estratégicos y de sus partes interesadas, mediante la aplicación del árbol de decisión propuesto en la Tabla 3.2.2.5

Respuesta	Explicación	Siguiente Pregunta
1. ¿Es el proceso de negocio una solución no estándar?		
SI	El sistema de Recaudo es la integración de un conjunto de componentes desarrollados específicamente para dar cumplimiento a lo dispuesto en la Ley Orgánica del Transporte Terrestre Transito y Seguridad Vial, respecto a "fomentar el principio de gestión empresarial por parte de las operadoras de transporte terrestre sustentado en los bondades que las Tecnologías de la Información y Comunicación".	Pregunta 2: ¿Interdependencias con los procesos de negocio?
2. ¿Es interdependiente con los procesos de negocio?		
SI	El principal beneficio del Sistema de Recaudo para la Agencia Nacional de Transito es supervisar y fiscalizar la aplicación de políticas tarifarias por parte de las operados de transito urbano de la provincia de Santa Elena, nada relacionado con los proceso de negocio de regulación y control del transporte terrestre, tránsito y seguridad vial.	Pregunta 3: ¿Diferencia de soluciones estándar basada en TI?
3. ¿Se diferencia de soluciones tradicionales basada en TI?		

SI	El sistema de Recaudo, se constituye en una solución innovadora y pionera en el mercado nacional que busca dotar a las operadoras del transporte urbano un sistema integrado que automatice las operaciones de recaudación tarifaria, mejorando la calidad del servicio de transporte público concesionado.	Pregunta 4: ¿Personalización de Aplicación/hardware/SO?
4. ¿Personalización de la software/plataforma/infraestructura?		
Yes	El sistema Recaudo al ser un conjunto de componentes y dispositivos de hardware, software, redes y seguridades interconectados entres sí, difícilmente podrá ser atendido por una solución de servicio por software (SaaS), donde toda la gestión de administración, replicación y respaldos, están restringidos para el usuario de nube, por lo que es necesario establecer cuál de las dos soluciones restantes mejor se ajusta a las necesidades de la Agencia Nacional de Tránsito.	Pregunta 5: ¿Personalización de Hardware/SO?
5. ¿Personalización de plataforma/infraestructura?		
Yes	Considerando que el sistema Recaudo al ser una solución hecha a la medida de la Agencia Nacional de Tránsito, requiere de configuraciones especificas a nivel de sistemas operativos y base de datos, las cuales se encuentra limitados en el modelo de servicio por Plataforma, por lo que es necesario establecer si la opción restante (IaaS) satisface los requerimientos del negocio,	Pregunta 6: ¿Personalización de Hardware?
6. ¿Personalización de Infraestructura?		
Yes	El modelo Infraestructura como Servicio (IaaS), se vislumbra como la mejor alternativa para la implementación del sitio alterno o contingencia del Sistema Central del Sistema Recaudo, sin embargo, cabe indicar que dicha solución no garantiza la replicación con el sitio principal y sus dispositivos (equipamiento abordo, red de distribución y módulos de atención al usuario) frente a una eventual caída cuyos costos deberán ser asumidos por la Agencia Nacional de Transito, al igual que los costos relacionados con firewall y respaldos especializados, protección de red y web, auditoria, monitoreo y balanceo de carga, semejante al configurado para el sitio principal. Por tanto se elimina a la Computación en la Nube como una solución viable para la implementación del sitio alterno del Sistema Recaudo debido al alto costo elevado que implicaría.	Solución: La computación en nube puede no ser la mejor solución para sus necesidades de negocio actuales.

Tabla 3.2.2.5: Aplicación árbol de decisión modelo de servicios.

De los resultados obtenidos en la Tabla 3.2.2.5, se evidencia que la Computación en la Nube no es la mejor solución para la puesta en marcha del sitio alterno o contingencia de Sistema Central del Sistema Recaudo, debido a los altos costos (costos ocultos), que implicaría implementar y/o replicar el esquema bajo el cual se encuentra operando el sitio principal (configuración de hardware), mismo que fue analizado en el paso 1. En todo caso, será la alta directiva quien disponga ir o no

por una Solución de Nube, independientemente del alto costo que esto implicaría para la Agencia Nacional de Tránsito. Proceso esquematizado en la Figura 3.2.2.7.

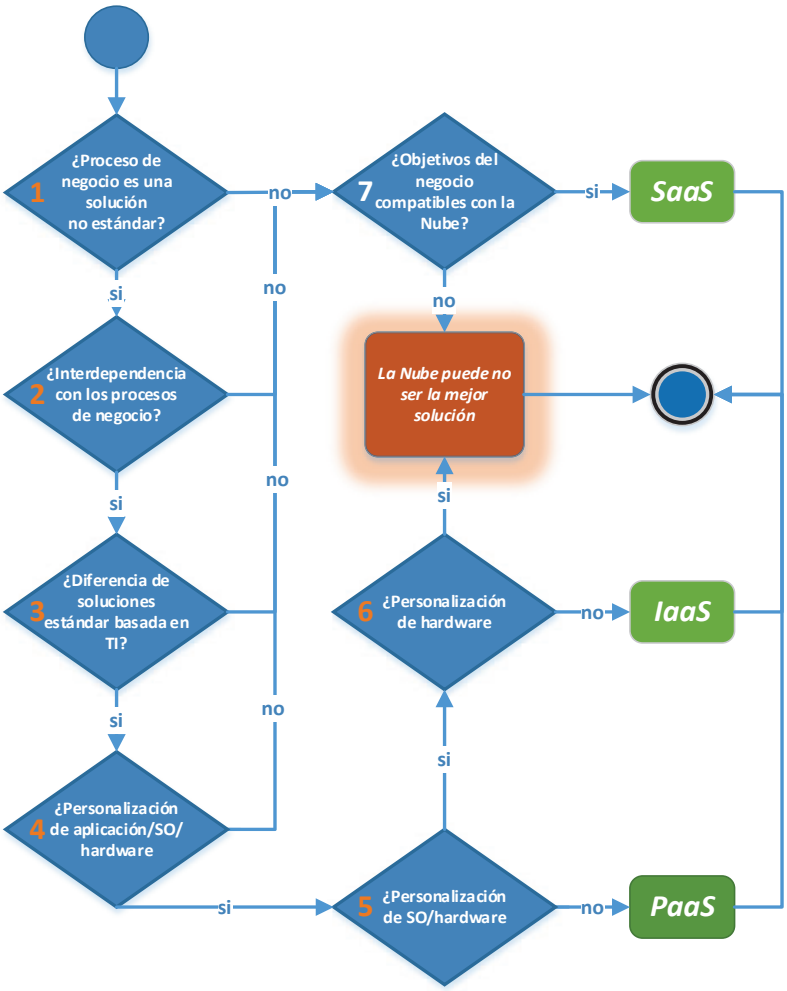

Figura 3.2.2.7 Árbol de decisión por Modelo de Servicio en la Nube

3.2.2.3 Paso 3: Selección del Modelo de Despliegue de Nube

Semejante al proceso de selección del modelo de servicio se puede ejecutar de manera paralela el árbol de decisión propuesto en la Tabla 2.2.3.3**¡Error! No se encuentra el origen de la referencia.**, a fin de identificar el modelo de despliegue que mejor se alinea con los objetivos estratégicos de la Agencia Nacional de Tránsito, garantizando la integridad, confidencialidad y disponibilidad del Sistema Central del "Sistema Integrado de Recaudación del Transporte Público Urbano de los cantones de Santa Elena, la Libertad y Salinas, en la Nube". Los resultados de la aplicación del árbol de decisión propuesto se resumen en la Tabla 3.2.2.6.

Respuesta	Explicación	Siguiente Pregunta
1. ¿Información sensible?		
No	Si los datos no son sensibles, entonces de los primeros pasos hacia la nube. Pese a que el Sistema Integrado de Recaudación Recaudo, maneja información sensible de los ciudadanos de la Provincia de Santa Elena, ésta se encuentra protegida mediante los mecanismos de encriptación de datos y definición de derechos de acceso propios del sistema, bajo estas consideraciones se puede dar los primeros pasos hacia la Nube.	***Pregunta*** 2: ¿Información Crítica?
2. ¿Información Crítica?		
Si	Los datos críticos pueden ser: • Planos • Fórmulas • Secretos comerciales • Cualquier información que sea absolutamente necesario para que la organización funcione Los datos críticos pueden ser colocados en la nube cuando los controles necesarios para protegerlos están en su lugar y funcionando con eficacia. Es importante señalar, sin embargo, que algunos de estos controles puede ser costoso y complejo, lo que puede aumentar el costo de trasladarse a la nube. El sistema central es considerado crítico, ya que es la parte medular del Sistema Integrado de Recaudación Recaudo, por tanto es necesario incorporar una serie de controles que permitan garantizar la disponibilidad del sistema, que por lo general no están embebidos en las soluciones de nube estándar y que su implementación requieren costos adicionales.	***Pregunta*** 14: ¿SLA?
14. ¿SLA?		
No	Si un SLA adecuada no puede ser acordado, trasladarse a la nube podría representar un nivel inaceptable de riesgo. Si el costo de la SLA es mayor que los beneficios del negocio, la solución de nube puede no ser la mejor solución.	***Solución***: Nube completa puede no ser la mejor solución. Una solución de nube Hibrida puede ser considerada.

Tabla 3.2.2.6: Aplicación árbol de decisión modelo de despliegue.

De los resultados obtenidos en la Tabla 3.2.2.6, se ratifica que la Computación en la Nube no es la mejor solución para la puesta en marcha del sitio alterno o contingencia de Sistema Central del Sistema Recaudo, debido a los altos costos que implicaría la implementación de mecanismos, herramientas y soluciones de aseguramiento de la información, como el cifrado y encriptación, que garanticen el acceso y disponibilidad del sistema. A esto debe sumarse, la imposición de los Acuerdos de Nivel de Servicio por parte del Proveedor de Servicio, cuyo porcentaje de satisfacción irá de la mano con el costo. En la Figura 3.2.2.8, se esquematiza el flujo del proceso de selección del modelo de despliegue.

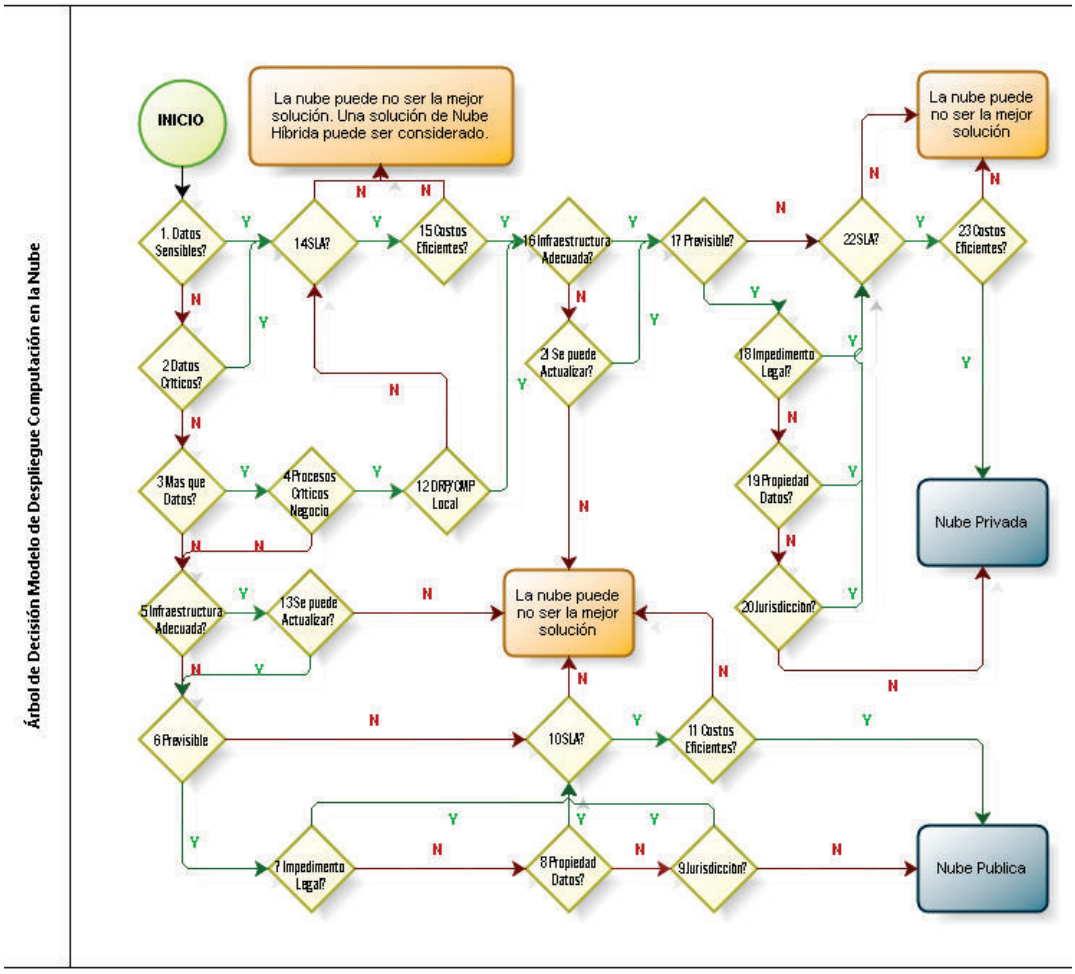

Figura 3.2.2.8 Árbol de decisión por Modelo de Despliegue en la Nube

3.2.2.4 Paso 4: Selección del Proveedor de Servicios de Nube

Independientemente de los resultados obtenidos en los numerales 3.2.2.2 y 3.2.2.3, en los que se corrobora que debido a la criticidad y los altos costo la Computación en la Nube no es la mejor solución para el “Sistema Integrado de Recaudación del Transporte Público Urbano de los cantones de Santa Elena, la Libertad y Salinas”, la Dirección de Tecnologías de la Información realizó un acercamiento con dos importantes proveedores de soluciones de conectividad, internet y centro de datos en el país, uno público y otro privado, que cumplen con la normativa local vigente en especial con el acuerdo ministerial 166 de la Secretaria Nacional de la Administración Pública, y que cuentan con certificación ISO/IEC 27001, aplicados a sus procesos de “Venta e Instalación de Productos y Servicios” [64], lo que brinda

a sus líneas de negocios un nivel de seguridad razonable, al soportar el cuidado de la integridad, confidencialidad y disponibilidad de la información de sus cliente.
Sin embargo, considerando que actualmente todas las soluciones de conectividad, internet y centro de datos con la que cuenta la Agencia Nacional de Tránsito se lo maneja a través de la Entidad Pública, se prevé que para la contratación de servicios en la Nube se acoja al Régimen Especial para la suscripción de contratos con Entidades Públicas.
Bajo estas consideraciones el presente análisis de selección del proveedor de servicio de Nube para el "Sistema Integrado de Recaudación del Transporte Público Urbano de los cantones de Santa Elena, la Libertad y Salinas", se lo realizó sobre la oferta Técnico – Económica [65] presentada por la Entidad Pública, al cual se incluye los Acuerdos de Nivel de Servicios [66], donde se evidencia lo siguiente:

- El modelo de servicios y el modelo de despliegue se ajustan al requerido: IaaS – Público.
- La oferta satisface los requerimientos de procesamiento, memoria y almacenamiento.
- La oferta no contempla aspectos de alta disponibilidad, redundancia y replicación, firewall robusto, dispersión geográfica y duplicación de datos (dentro del territorio nacional), soluciones de respaldo, de auditoría y de monitoreo.
- El acceso a los servicios de Nube a un se ven limitados por el Ancho de Banda, como responsabilidad del usuario.
- Los Acuerdos de Nivel de Servicios no son específicos para los Servicios de Computación en la Nube, engloba todo el portafolio de servicios del proveedor (enlaces de datos, internet, centro de datos).
- Para el cálculo de la Disponibilidad de Servicio de Nube aún se contemplan los mantenimientos preventivos planificados, los atentados, el hurto y el vandalismo, como caso fortuito o fuerza mayor, que supuestamente con la Computación en la Nube iban a ser mitigados.
- Seguridad y Ventajas de Escala.- La implementación de medidas de seguridad (filtrado, administración de parches, redundancia de hardware y software, firewall

empresarial, autenticación segura (soluciones federadas), ubicaciones múltiples) tienen un costo adicional.

- Interfaces normalizadas.- No se manejan interfaces abiertas y estandarizadas, lo que dificultaría el cambio a un nuevo proveedor, incurriendo en mayores gastos.
- Auditoría y recogida de pruebas.- No contemplado, lo que limita la identificación de incidentes de seguridad en vivo.

Por lo expuesto, es evidente que en el Ecuador aún no se cuenta con proveedores de servicios de Nube con la capacidad de garantizar el fiel cumplimiento de los valores, ventajas y beneficios tan anunciadas para la Computación en la Nube y tan requeridas para la implementación de la contingencia del "Sistema Integrado de Recaudación del Transporte Público Urbano de los cantones de Santa Elena, la Libertad y Salinas" en la Nube.

3.2.3 FASE III: GESTIÓN DE RIESGOS

Como resultados de la fase II, queda claro que pese a las buenas intenciones del directorio de la Agencia Nacional de Tránsito por adoptar la computación en la Nube como estrategia para reducir cotos e incrementar la productividad, no es procedente en un mercado ecuatoriano donde las soluciones de Nube no terminan por despegar. Más aún, si debido a normativas legales monopolizan el mercado de prestación de servicios a unos cuantos proveedores nacionales, quienes aún no se encuentran en la capacidad de garantizar y atender los requerimientos de seguridad planteados por las entidades gubernamentales, y si lo hacen es a un costo muy elevado que termina por exceder el presupuesto inicialmente planteado.

Sin embargo para fines didácticos de aplicación de la última fase del Modelo de Gestión de Riesgos de Infraestructura como Servicios (IaaS) de Cloud Computing aplicado a entidades del sector público ecuatoriano, se da por hecho la autorización de la alta directiva de la Agencia Nacional de Tránsito para la implementación de la contingencia del Sistema Central del "Sistema Integrado de Recaudación", en la Nube.

Del análisis realizado en los numeral 3.2.2.2 y 3.2.2.3, el modelo de servicios que mejor se adapta a las necesidades de la Agencia Nacional de Tránsito es

Infraestructura como Servicio (IaaS), mientras que el modelo de despliegue seleccionado es Nube Pública, la cual se ajusta a las capacidades del proveedor de Nube local.

Bajo esta premisa es necesario que la Dirección de Tecnologías de la Información en su calidad de proceso de apoyo a la gestión y consecución de objetivos y metas institucionales de los Procesos Gobernantes y Proceso Agregadores de Valor de la Agencia Nacional de Tránsito, desarrolle e implemente una eficiente y efectiva Gestión de Riesgos de Servicios en la Nube, que se alínee a los objetivos y niveles de tolerancia de riesgos establecidos por su directorio, antes de empezar con el proceso de implementación de la contingencia del Sistema Recaudo en la Nube, como el propuesto en la Figura 3.2.3.1.

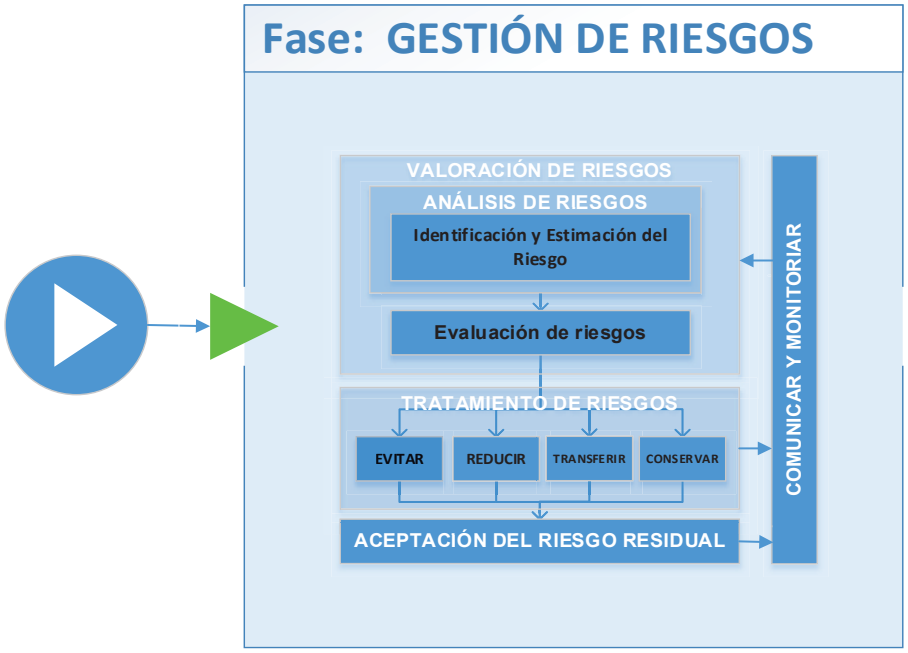

Figura 3.2.3.1 Gestión de Riesgos de Computación en la Nube

Metodología de Gestión de Riesgos de la Figura 3.2.3.1, que parte realizando una valoración del riesgo, para en base a ello determinar los posibles riesgos y su tratamiento frente a la probabilidad de impacto que causaría la materialización de uno de ellos. Finalmente, se proponen controles para mitigar los riesgos aceptados, los cuales deben ser comunicados a todo nivel organizacional y monitoreado permanentemente por parte del comité de gestión de riesgos de la ANT.

Cabe indicar que la ***etapa*** de aceptación del riesgo garantiza que los riesgos residuales son aceptados explícitamente por el Directorio de la Agencia Nacional de Tránsito, a fin de establecer responsabilidades en caso de que los controles sean omitidos o pospuestos.

3.2.3.1 Valoración del Riesgos

Toda vez que en el numeral 3.2.2, se estableciese que la alta disponibilidad del "Sistema Integrado de Recaudación del Transporte Público Urbano de los cantones de Santa Elena, la Libertad y Salinas" constituye un factor crítico de éxito, tanto para garantizar la movilidad de sus ciudadanos bajo los principios de seguridad, eficiencia, responsabilidad, universalidad, accesibilidad, continuidad y calidad, así como, para fomentar el principio de gestión empresarial por parte de sus operadoras a través del uso de las Tecnologías de la Información y Comunicación, se plantea una arquitectura de alta disponibilidad esquematizada en la Figura 3.2.3.2, donde el sitio alterno, caso de estudio, estaría en la Nube.

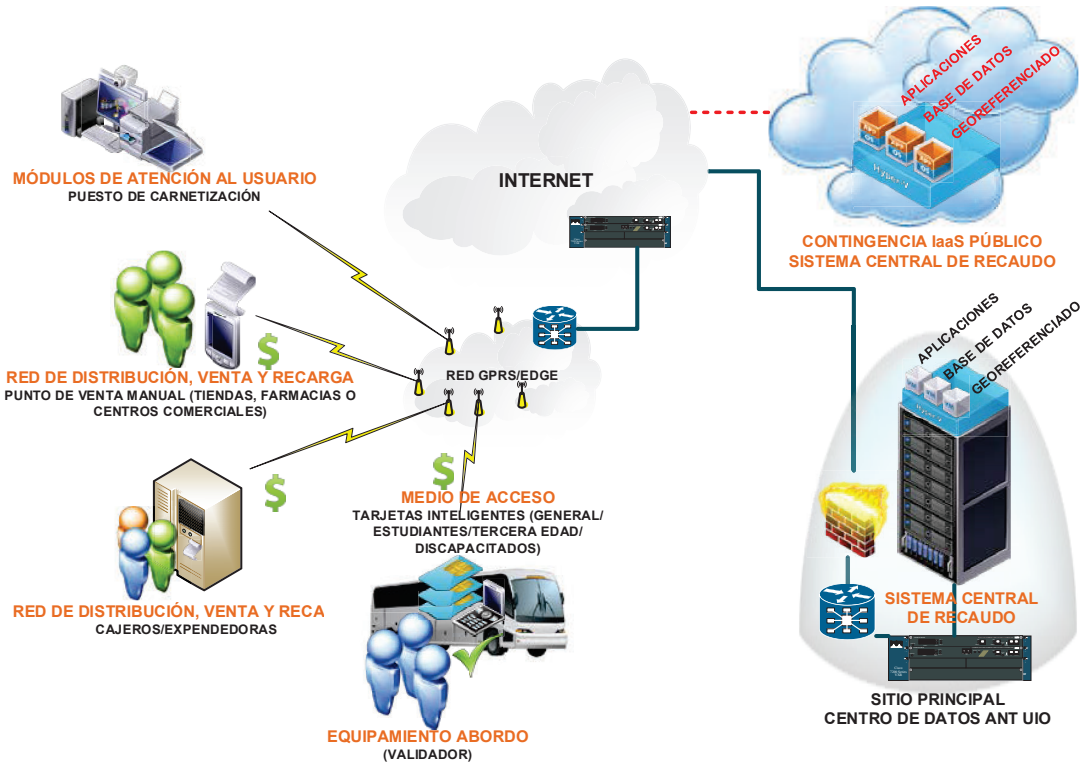

Figura 3.2.3.2 Alta disponibilidad (Nube) para el Sistema Recaudo

Por lo expuesto, es necesario realizar una valoración del riesgo que permita a la Dirección de Tecnologías de la Información, determinar el valor de los activos de Información, identificar las amenazas y vulnerabilidades aplicables que existen o que podrían existir, identificar los controles existentes y sus efectos en el riesgo identificado, determinar las consecuencias potenciales, para finalmente, priorizar los riesgos derivados y clasificarlos frente a los criterios de evaluación del riesgo.

3.2.3.1.1 Análisis de Riesgos.-

Considerando que un riesgo es la probabilidad de que una amenaza explote las vulnerabilidades de un servicio de Nube causando daño a la organización, más aún si no se cuenta con contramedidas vigentes para mitigarlas, es necesario que la Agencia Nacional de Tránsito en su camino a hacia la nube identifique las amenazas, vulnerabilidades y riesgos relacionados con el modelo de servicio y con el modelo de despliegue escogido.

Como parte inicial de esta etapa es necesario identificar las amenazas que pueden atentar contra la confidencialidad, integridad, disponibilidad, autentificación, autorización y auditoría del "Sistema Integrado de Recaudación del Transporte Público Urbano de los cantones de Santa Elena, la Libertad y Salinas", para lo cual se debe incorporar las amenazas identificadas en el numeral 1.2.1, con las amenazas identificadas en el análisis de fortalezas, oportunidades, debilidades y amenazas del numeral 3.2.2.1.5, como el propuesto en la tabla 3.2.3.1.1.

COD.	AMENAZA
A01	Espionaje de información sobre datos transmitidos o almacenados
A02	Transmisión de datos vulnerable
A03	Amenaza interna
A04	Objetivo atractivo para ataques con motivos políticos e impactos elevados
A05	Modificación no autorizada de información.
A06	Pérdida o fuga de información
A07	Mal funcionamiento o denegación del servicio.
A08	Problemas derivados de las tecnologías compartidas
A09	Deterioro del rendimiento por compartición de recursos
A10	Disminución de la velocidad de acceso por implementación de sistemas o protocolos seguros o por mala configuración de los mismos
A11	Suplantación de identidad o burla sobre los sistemas de identificación.
A12	Secuestro de sesión o servicio
A13	Acceso no autorizado al sistema e información.
A14	Interfaces y API poco seguros

A15	Riesgos por desconocimiento
A16	Destrucción de logs, registros y bitácoras.
A17	Dificultad para acceder a registros y/o datos de auditoria (Informática forense)
A18	Aprovechar errores en contratos o acuerdos de nivel de servicio.
A19	Abuso y mal uso del cloud computing
A20	Dificultad para transferir datos de vuelta al usuario o proveedor alternativo elegido, por adopción de formato propietario para almacenar datos.
A21	Ausencia de normativa legal local que regule la prestación de servicios en la Nube
A22	*Perfil de riesgo desconocido*
A23	Proveedores no certificados en estándares de Seguridad de la Información.
A24	Monopolio por parte de pocos proveedores que pueden brindar el servicio de Nube.
A25	La confiabilidad de los servicios depende de la salud tecnológica y financiera del proveedor.
A26	Mercado inmaduro y no posesionado a nivel gubernamental.
A27	Entidades gubernamentales con asignación presupuestaria para TI holgada, que genera reticencia en la adopción de nube por contar con Centro de Datos Propios e infraestructura tecnológica de punta.
A28	Costos elevados si se desea garantizar los tres pilares fundamentales de la seguridad de la información, sin contar la alta disponibilidad, replicación y recuperación de desastres.

Tabla 3.2.3.1.1: Identificación de Amenazas

Para el caso específico de la computación en la nube, las amenazas de la tabla 3.2.3.1.1 están expuestas a un cambio continuo y tienen su origen en el proveedor de Nube.

Luego, de identificar las amenazas es necesario la identificación de vulnerabilidades que pueden ser explotadas por las amenazas antes descritas para causar daños al “Sistema Integrado de Recaudación del Transporte Público Urbano de los cantones de Santa Elena, la Libertad y Salinas” y por ende a la Agencia Nacional de Tránsito. En la Tabla 3.2.3.1.2, se identifican dichas vulnerabilidades, cuyo detalle se encuentra en el anexo 5.

COD.	VULNERABILIDADES
V01	Falta de tecnologías y soluciones estándar
V02	Selección de proveedores insuficiente
V03	Ausencia de redundancia de suministrador
V04	Falta de integridad y transparencia en los términos de uso
V05	Funciones y responsabilidades confusas
V06	Aplicación deficiente de las definiciones de funciones
V07	Sincronización de las responsabilidades o las obligaciones contractuales externas a la nube
V08	Cláusulas SLA con compromisos en conflicto para con diferentes partes.
V09	Auditoría o certificación no disponible para los clientes
V10	Aplicaciones inter-nube que crean dependencia oculta
V11	Almacenamiento de datos en jurisdicciones múltiples
V12	Almacenamiento de datos en jurisdicciones múltiples y falta de transparencia sobre este punto

V13	Falta de transparencia
V14	Ausencia de un acuerdo de depósito de fuentes
V15	Falta de control en el proceso de evaluación de vulnerabilidad
V16	Sistemas de certificación no adaptados a las infraestructuras de nube
V17	Falta de información sobre jurisdicciones
V18	Ausencia de aislamiento de los recursos
V19	Ausencia de aislamiento de los recursos Software que no es de confianza
V20	Falta de aislamiento de la reputación
V21	Vulnerabilidades del hipervisor
V22	Modelado inadecuado del uso de recursos.
V23	Provisión de recursos e inversiones en infraestructura inadecuadas.
V24	Ausencia de políticas de limitación de recursos
V25	Posibilidad de que se realice un análisis interno de la red (en nube)
V26	Posibilidad de que se realicen comprobaciones de corresidencia
V27	No aplicación del principio de «need-to-know»
V28	Vulnerabilidades AAA
V29	Vulnerabilidades del sistema o del sistema operativo
V30	Procedimientos de seguridad física inadecuados
V31	Imposibilidad de procesar datos codificados.
V32	Vulnerabilidades de la aplicación o gestión de parches insuficiente
V33	Acceso remoto a la interfaz de gestión
V34	Configuración deficiente
V35	Vulnerabilidades en la codificación de la comunicación
V36	Falta o debilidad en la codificación de archivos y datos en tránsito
V37	Limpieza de medios sensibles
V38	Recursos de filtrado inadecuados o mal configurados
V39	Vulnerabilidades del alta de usuarios
V40	Vulnerabilidades de la baja de usuarios
V41	Procedimientos insuficientes de gestión de claves
V42	Generación de claves: Baja entropía para la generación de números aleatorios
V43	Software que no es de confianza
V44	Ausencia de conciencia de seguridad
V45	Responsabilidad por pérdida de datos
V46	Ausencia de disponibilidad experta
V47	Pérdida o robo de las copias de seguridad

Tabla 3.2.3.1.2: Identificación de Vulnerabilidades

En general las vulnerabilidades identificadas en la Tabla 3.2.3.1.2, por si solas no causan daño, requieren de una amenaza para explotarla. Por el contrario una amenaza que no tiene una vulnerabilidad no necesariamente puede resultar en un riesgo, por lo tanto es recomendable conocer y monitorear permanentemente las vulnerabilidades para determinar los cambios.

Una vez identificadas las amenazas y vulnerabilidades que puede afectar al "Sistema Integrado de Recaudación" en la Nube, es necesario confrontarlas entre sí a fin de identificar un conjunto de riesgos como el listados en la Tabla 3.2.3.1.3, los cuales parten del propuesto en el numeral 1.2.2.

AMENAZAS	VULNERABILIDADES	COD.	RIESGOS
A07, A08, A09, A10, A24, A25	V01, V02, V03, V04	R01	Vinculación
A18, A19, A20, A21, A24, A25, A27	V01, V04, V05, V06, V07, V08, V09, V10, V11, V12, V13, V14, V15	R02	Pérdida de gobernanza
A07, A08, A09, A10, A23, A26	V01, V04, V09, V11, V14, V15, A28	R03	Desafíos de cumplimiento
A01, A02, A03, A04, A07, A08, A09, A10	V16, V17, V18	R04	Pérdida del renombre empresarial a raíz de actividades de prestación conjunta
A07, A08, A09, A10, A23, A24,	V03, V19, V20, V21, A28	R08	Agotamiento de recursos (prestación excesiva o insuficiente)
A01, A02, A03, A04, A07, A08, A09, A10, A23, A24	V16, V17, V18, V22, V23, A28	R09	Fallo de aislamiento
Todas	V05, V06, V24, V25, V26, V27, V28, V29	R10	Miembros maliciosos de proveedores en nube. Abuso de funciones privilegiadas
A01, A02, A03, A04, A07, A08, A09, A10	V25, V26, V29, V30, V31	R11	Compromiso de interfaz de gestión (manipulación, disponibilidad de la infraestructura)
A01, A02, A03, A04, A07, A08, A09, A10	V04, V22, V23, V25, V32, V33	R12	Interceptación de datos en tránsito
A01, A02, A03, A04, A07, A08, A09, A10, A11, A12, A13, A14, A15	V04, V22, V23, V25, V32, V33	R13	Fuga de datos durante la carga/descarga dentro de la nube
A07, A08, A09, A10, A18, A19, A20, A21	V34	R14	Supresión de datos insegura o ineficaz
A07, A08, A09, A10	V26, V31, V35	R15	Distribución de denegación de servicio (DDoS)
A01, A02, A03, A04, A05, A06, A07, A08, A09, A10	V22, V23	R18	Realización de escaneados o detecciones maliciosas
A07, A08, A09, A10, A18, A19, A20, A21, A23	V11, V15, V16	R21	Órdenes judiciales y descubrimiento electrónico
A01, A02, A03, A04, A05, A06, A07, A08, A09, A10, A23	V11, V15	R23	Riesgos de la protección de datos
A01, A02, A03, A04, A05, A06, A07, A08, A09, A10	V16, V26, V31	R25	Brechas en la red
A01, A02, A03, A04, A05, A06, A07, A08, A09, A10	V16, V26, V31, V40	R26	Gestión de la red (congestión de la red/fallo en la conexión/uso no óptimo)
A01, A02, A03, A04, A05, A06, A07, A08, A09, A10	V13, V32, V36, V37	R27	Modificación del tráfico de la red

A01, A02, A03, A04, A11, A12, , A13, A14, A15	V05, V06, V18, V24, V25, V31, V36, V37	R28	Escalada de privilegios
A01, A02, A03, A04, A11, A12, , A13, A14, A15	V16, V27, V32, V36, V41	R29	Ataques de ingeniería social (suplantación)
A16, A17, A18, A19, A20, A21	V25, V26, V36, V37, V42, V43	R30	Pérdida o compromiso de los registros operativos
A16, A17, A18, A19, A20, A21	V25, V26, V36, V37, V42, V43, V44	R31	Pérdida o compromiso de los registros de seguridad (manipulación de la investigación experta)
A01, A02, A03, A04, A05, A06, A07, A08, A09, A10	V25, V27, V36, V37	R32	Pérdida o robo de las copias de seguridad
A03, A05, A13	V27, V30	R33	Acceso no autorizado a los locales (incluido el acceso físico a las máquinas y otras instalaciones)
A23	V40	R35	Catástrofes naturales

Tabla 3.2.3.1.3: Identificación de Riesgos.

3.2.3.1.2 Evaluación de Riesgos.

Basado en una estimación cualitativa de experiencias de entidades gubernamentales que implementaron la Computación en la Nube y de casos de estudios de entidades internacionales como la CSA, a continuación se realiza una evaluación de aquellos riesgos considerados como críticos o importantes. Estimación Cualitativa seleccionada considerando que es menos compleja y menos costosa que una estimación cuantitativa, y que brinda a la Agencia Nacional de Tránsito una valoración detallada de los riesgos relacionados con la Computación en la Nube, al incluir la valoración de las amenazas y vulnerabilidades identificadas en el numeral 3.2.3.1.1.

Para la evaluación cualitativa de riesgos de servicios en la Nube se emplea la matriz E1 de la ISO/IEC27005, que resulta de la consideración de la probabilidad de un escenario de incidentes, graficado frente al impacto estimado en el negocio. El escenario del incidente vendrá dado por una amenaza que explota una vulnerabilidad con una probabilidad determinada. En la Tabla 3.2.3.1.4, se resume los niveles de riegos para la implementación del “Sistema Integrado de Recaudación del Transporte Público Urbano de los cantones de Santa Elena, la Libertad y Salinas”, bajo el modelo de IaaS-Público. Donde el riesgo resultante se mide en una escala de 0-8 (Riesgo Bajo: 0 -2; Riesgo Medio: 3-5; Riesgo Alto: 6-8) que se puede evaluar frente a los criterios de aceptación del riesgo.

	Probabilidad del escenario de incidente	Muy baja (Muy improbable)	Baja (Improbable)	Media (Posible)	Alta (Probable)	Muy alta (Frecuente)
Impacto en el Negocio	Muy baja					
		0	*1*	*2*	*3*	*4*
	Baja			R18		R22
		1	*2*	*3*	*4*	*5*
	Media		R06, R07, R20, R30, R31,	R08, R24		R01, R21
		2	*3*	*4*	*5*	*6*
	Alta	R16, R17, R33, R34, 35	R04, R08, R27, R28, R32	R12, R13, R15, R29	R23	R03
		3	*4*	*5*	*6*	*7*
	Muy alta	R5, R19	R25	R09, R10, R11, R14, R26,		R02
		4	*5*	*6*	*7*	*8*

Tabla 3.2.3.1.4: Resultado estimación de riesgos.

A continuación se evalúan aquellos riesgos de la Tabla 3.2.3.1.3, calificados como Riesgos Altos, para lo cual es necesario organizarlos por categorías (Políticas/Organizativas, Técnicas y Operativas) y tener presente lo siguiente:

- **RIESGOS ORGANIZATIVOS Y/O POLÍTICOS**

  - ***R01: Vinculación***.- De acuerdo a la propuesta del proveedor de Nube, éste ofrece a la Agencia Nacional de Tránsito herramientas, procedimientos, formatos de datos e interfaces propietarias, los cuales no garantizan la portabilidad o compatibilidad con la Infraestructura virtual que maneja la ANT, que en el caso de querer retornar hacia la infraestructura local o a otro proveedor de Nube se enfrentaría a una tarea difícil, compleja y a menudo costosa, pues de cierta forma estará atada al proveedor inicial. y pareciese que el modelo propuesto por el proveedor fue diseñado con esta intensión.

    Dependencia perjudicial a la imagen corporativa de la Agencia Nacional de Tránsito en su afán de garantizar la alta disponibilidad del Sistema Recaudo al servicio de la ciudadanía de la Provincia de Santa Elena. Adicionalmente el tipo de almacenamiento y herramientas de seguridad contempladas en la oferta son básicos o limitados, que no garantizan los niveles de seguridad requeridos por la ANT, lo que plantea un escenario de pánico bancario, donde llegado el caso y debido a la limitada cantidad y plazo para la retirada de información, es vuelve una tarea titánica.

Probabilidad	**Alta**	**Comparativa: Mas Alta**
Impacto	Medio	Comparativa: Igual
Amenazas	**Mal funcionamiento o denegación del servicio.** Deterioro del rendimiento del sistema debido a compartición de recursos Disminución de la velocidad de acceso por implementación de sistemas y/o protocolos seguros o por mala configuración de los mismos La confiabilidad de los servicios depende de la salud tecnológica y financiera del proveedor. Monopolio por parte de pocos proveedores que pueden brindar el servicio de Nube.	
Vulnerabilidades	Falta de tecnologías y soluciones estándar en el país. Selección de proveedores nacionales insuficiente (Monopolio) Falta de integridad y transparencia en los términos de uso Limitación a tecnologías dada por el Proveedor	
Activos Afectados	Renombre de la ANT. Disponibilidad del Sistema Recaudo.	
Controles	Incorporar mecanismos en el contrato y en los acuerdos de nivel de servicios que permitan controlar los procesos y controles para la portabilidad de la data por parte del proveedor, evitando el supuesto pánico bancario. Comprender las tecnologías que sustentan la infraestructura del proveedor para comprender y mitigar las implicaciones de dependencia, privacidad y seguridad. Asegurarse que durante una interrupción prolongada del servicio, las operaciones críticas se pueden reanudar inmediatamente y todo el resto de operaciones, en un tiempo prudente.	
Recomendaciones	Diseñar buenas prácticas para la instalación y configuración Monitorizar los entornos para detectar cambios no deseados en las configuraciones o la actividad Proporcionar autenticación fuerte y control de acceso para el acceso de administración Adecuar los acuerdos de nivel de servicio para controlar el parcheado y la corrección de vulnerabilidades	
Riesgos	Alto	

Tabla 3.2.3.1.5: Evaluación riesgos de vinculación o dependencia del proveedor.

- ***R2: Pérdida de Control y/o Gobernabilidad***.- Supuestamente, con la migración a la Nube se debería dividir responsabilidades entre la Agencia Nacional de Tránsito y el proveedor, sin embargo, el no tener claro cuales corresponden a cada quien, peor aún si no se especifica en el contrato o acuerdos de nivel de servicio, da pie a omisión y a no tener responsables en caso de un evento negativo. Esta supuesta cesión de obligaciones no exime a la ANT realizar un monitoreo de las actividades efectuadas por el proveedor, quien podría generar un agujero de seguridad si toma ciertas acciones como: no realizar los procedimientos, realizarlos

inadecuadamente, o delegarlos a empresas desconocidas, lo cual no ofrece garantías desde el punto de vista legal.

De igual forma, el proveedor puede subcontratar o externalizar servicios a terceros (firewall, backup, alta disponibilidad) que podrían no ofrecer las mismas garantías ofrecidas por el proveedor en nube, o que se produzcan cambios en el control del proveedor en nube de modo que provoquen una modificación de los términos y condiciones de sus servicios.

Por lo tanto, la pérdida de gobernanza y control, podría repercutir gravemente sobre la estrategia de la Agencia Nacional de Tránsito en el cumplimiento de su misión y objetivos.

Probabilidad	**Muy Alta**	**Comparativa: Mas Alta**
Impacto	Muy Alto	Comparativa: Igual
Amenazas	**Aprovechar errores en contratos o acuerdos de nivel de servicios** Perfil de riesgo desconocido Proveedores no certificados en estándares de Seguridad de la Información x Aprovechar errores en contratos o acuerdos de nivel de servicio. Abuso y mal uso del cloud computing Ausencia de normativa legal local que regule la prestación de servicios en la Nube Amenaza interna Modificación no autorizada de información. Acceso no autorizado al sistema e información. Riesgos por desconocimiento	
Vulnerabilidades	Funciones y responsabilidades confusas por parte del Proveedor Aplicación deficiente de las definiciones de funciones Sincronización de las responsabilidades o las obligaciones contractuales externas a la nube Cláusulas SLA con compromisos en conflicto para con diferentes partes Auditoría o certificación no disponible para los clientes Aplicaciones inter-nube que crean dependencia oculta Falta de tecnologías y soluciones estándar Falta de control en el proceso de evaluación de vulnerabilidad Sistemas de certificación no adaptados a las infraestructuras de nube Falta de integridad y transparencia en los términos de uso Propiedad de los activos confusa	
Activos Afectados	Renombre de la ANT. Disponibilidad del Sistema Recaudo. Confianza del cliente	
Controles	Implantar políticas y estándares en la provisión de servicios en la Nube. Establecer mecanismos de auditoría y herramientas para que se sigan las políticas de la organización durante el ciclo de vida.	
Recomendaciones	Especificar cláusulas legales y de confidencialidad en los contratos laborales	

	Determinar los posibles problemas en los procesos de notificación Aplicar técnicas de autenticación de doble factor siempre que sea posible Monitorizar las sesiones en busca de actividades inusuales proporcionar autenticación fuerte y control de acceso para el acceso de administración Adecuar los acuerdos de nivel de servicio para controlar el parcheado y la corrección de vulnerabilidades
Riesgos	Alto

Tabla 3.2.3.1.6: Evaluación riesgos de pérdida de control o gobernabilidad

- ***R3: Desafío de Cumplimiento***.- La Agencia Nacional de Tránsito realizó una inversión alta en la adquisición del "Sistema Integrado de Recaudación del Transporte Público Urbano de los cantones de Santa Elena, la Libertad y Salinas", el cual cumple con normas o estándares internacionales para gestión de la calidad y seguridad, misma que le brinda cierta ventaja competitiva en el mercado. Esta transición a la Nube pone en riesgos tales certificaciones, más aún, si el potencial proveedor de servicios no permite una auditoría externa para validarlos. Adicionalmente, respecto a futuros procedimientos judiciales, la solución de nube propuesta dificultan el cumplimiento de las obligaciones de la ANT ya que no contempla la preservación o almacenamiento de metadatos originales como fechas de creación y/o modificación.

Probabilidad	**Muy Alta**	**Comparativa: Mas Alta**
Impacto	Alto	Comparativa: Igual
Amenazas	**Aprovechar errores en contratos o acuerdos de nivel de servicios** Mal funcionamiento o denegación de servicios Proveedores no certificados en estándares de Seguridad de la Información Ausencia de normativa legal local que regule la prestación de servicios en la Nube	
Vulnerabilidades	Falta de tecnologías y soluciones estándar Falta de integridad y transparencia en los términos de uso Auditoría o certificación no disponible para los clientes. Sistemas de certificación no adaptados a las infraestructuras de nube Falta de certificación en procedimientos o normas internacionales (gobierno, calidad y seguridad)	
Activos Afectados	Confianza del cliente Certificación	
Controles	Revisar y valorar las medidas del proveedor con respecto a las necesidades de la organización. Entender los distintos tipos de leyes y regulaciones y su impacto potencial en los entornos de Nube. Implementación de salvaguardas técnicas, físicas y administrativas, como el cifrado de los datos por parte de la ANT.	

Recomendaciones	Estar al corriente, total o parcialmente, de los detalles de la infraestructura Monitorizar y recibir alertas sobre el uso de información crítica
Riesgos	Alto

Tabla 3.2.3.1.7: Evaluación riesgos de cumplimiento

- **RIESGOS TÉCNICOS**

  - ***R9: Fallo de Aislamiento***.- El hecho de compartir recursos distribuidos tales como, almacenamiento, procesamiento o comunicación, es uno de los riesgos que más preocupa a la Agencia Nacional de Tránsito, ya que en la propuesta presentada por el proveedor no garantiza una provisión dinámica del servicio ni el aislamiento de los suscriptores del servicio, lo que da a entender que la concurrencia de usuarios del proveedor se realizará mediante la multiplexación de varias máquinas virtuales sobre un mismo servidor físico, constituyéndolos en foco de ataque, en caso de que los mecanismos de aislamiento no funcionen correctamente y un usuario se aproveche esto para violar la confidencialidad, integridad o disponibilidad de los sistemas de sus vecinos. Para el caso de una infraestructura de nube pública la probabilidad que se produzca es alta.

Probabilidad	**Media**	**Comparativa: Mas Alta**
Impacto	Muy Alto	Comparativa: Mas Alta
Amenazas	Espionaje de información sobre datos transmitidos o almacenados. Modificación no autorizada de información. Mal funcionamiento del sistema o denegación de servicio. Objetivo atractivo para ataques con motivos políticos e impactos elevados Pérdida o fuga de información Problemas derivados de las tecnologías compartidas Deterioro del rendimiento por compartición de recursos Disminución de la velocidad de acceso por implementación de sistemas o protocolos seguros o por mala configuración de los mismos Monopolio por parte de pocos proveedores que pueden brindar el servicio de Nube. Adopción de formatos propietarios para almacenar información.	
Vulnerabilidades	Vulnerabilidades del hipervisor Ausencia de aislamiento de los recursos Falta de aislamiento de la reputación Posibilidad de que se realice un análisis interno de la red (en Nube) Posibilidad de que se realicen comprobaciones de corresidencia Sistema débil de autenticación y autorización. Error en algoritmos de asignación de recursos.	
Activos Afectados	Renombre de la ANT. Disponibilidad del Sistema Recaudo. Perdida de datos sensibles.	

	Confianza del cliente
Controles	El proveedor de Nube debe garantizar que la información estará correctamente aislados y que los procedimientos de cifrado de la información se realizarán por personal experimentado, ya que el cifrado de los datos mal realizado también puede producir problemas con la disponibilidad de los datos o incluso la pérdida de los mismos. Se deben conservar los registros detallados de las actividades internas, el proveedor debe adoptar políticas de rotación de empleados y también se deben adoptar políticas de «need-to-know». Desde la perspectiva del hipervisor la Agencia Nacional de Tránsito debe entender la virtualización y otras técnicas de aislamiento que el proveedor emplee y valorar los riesgos implicados.
Recomendaciones	Diseñar buenas prácticas para la instalación y configuración. Monitorizar los entornos para detectar cambios no deseados en las configuraciones o la actividad. Proporcionar autenticación fuerte y control de acceso para el acceso de administración Monitorizar el tráfico para la detección de posibles actividades ilícitas Comprobar las listas negras públicas para identificar si los rangos IP de la infraestructura han entrado en ellas Analizar los problemas de seguridad de las interfaces de los proveedores de servicio. Asegurarse que la autenticación y los controles de acceso se implementan teniendo en cuenta el cifrado de los datos
Riesgos	Alto

Tabla 3.2.3.1.8: Evaluación riesgos de aislamiento.

- ***R10: Miembros Maliciosos o Abuso de Funciones Privilegiadas***.- Las vulnerabilidades a nivel de proveedor pueden afectar sobre la confidencialidad, integridad y disponibilidad del Sistema Recaudo de la Agencia Nacional de Tránsito, más aún, si la solución propuesta no contempla métodos de autenticación y control de acceso seguros, tan requeridos para el modelo de servicio escogido (IaaS), donde el proveedor de nube se encarga de la infraestructura de hardware.

Probabilidad	**Media**	**Comparativa: Mas Alta**
Impacto	Muy Alto	Comparativa: Mas Alta
Amenazas	Amenaza interna Modificación no autorizada de información. Suplantación de identidad o burla sobre los sistemas de identificación Acceso no autorizado al sistema e información. Interfaces y API poco seguros Riesgos por desconocimiento Abuso y mal uso del cloud computing Perfil de riesgo desconocido	
Vulnerabilidades	Funciones y responsabilidades confusas.	

	Aplicación deficiente de las definiciones de funciones No aplicación del principio de «need-to-know» Vulnerabilidades AAA Vulnerabilidades del sistema operativo Procedimientos de seguridad física inadecuados Imposibilidad de procesar datos codificados Vulnerabilidades de la aplicación Gestión de parches insuficiente
Activos Afectados	Renombre de la ANT. Disponibilidad del Sistema Recaudo. Perdida de datos sensibles. Confianza del cliente Control de acceso, autenticación y/o autorización.
Controles	Asegurar las salvaguardas necesarias para hacer seguras la autenticación, la autorización y las funciones de control de acceso. Consensuar con el proveedor los usuarios que tendrán acceso a la infraestructura del Sistema Recaudo, para minimizar así los riesgos de que haya usuarios con elevados privilegios que no deberían tener acceso a los datos.
Recomendaciones	Especificar cláusulas legales y de confidencialidad en los contratos. Determinar los posibles problemas en los procesos de notificación. Proporcionar autenticación fuerte y control de acceso para el acceso de administración. Implementar API potentes para el control de acceso Definir, por contrato, el establecimiento de roles y funciones a nivel de proveedor. Prohibir, mediante políticas, compartir credenciales entre usuarios y servicios Aplicar técnicas de autenticación de doble factor siempre que sea posible Monitorizar las sesiones en busca de actividades inusuales Monitorizar y recibir alertas sobre el uso de información crítica
Riesgos	Alto

Tabla 3.2.3.1.9: Evaluación riesgos de funciones privilegiadas.

- **RIESGOS LEGALES**

  - ***R21: Problemas de Jurídicos y Políticas***.- Dada la criticidad del Sistema Integrado de recaudación para la Agencia Nacional de Tránsito, ésta no puede acarrear pérdidas o falencias (Internas o externas). En tales casos la primera acción será recurrir a las políticas de operación y acuerdos de nivel de servicio para entablar una solicitud de reclamación fundamentada, sin embargo, dada la imposición por parte del proveedor de dichas políticas y acuerdos de servicio que en su mayoría no cubre todos los escenarios de riesgos, esto se convierte en un problema latente pues no hay punto de reclamación, y en tal caso la segunda instancia es acudir a políticas y leyes de estado, pero, dado que los servicios de Nube en el Ecuador aun no son

normados o regulados, dejan a la ANT sin argumentos para reclamar sus derechos. A lo que se debe incorporar los riesgos relacionados con investigación electrónica fruto de una orden judicial o demandas civiles sobre la infraestructura de nube del proveedor, lo que puede atentar gravemente contra la confidencialidad de la información de sus clientes.

Probabilidad	**Alta**
Impacto	Medio
Amenazas	Aprovechar errores en contratos o acuerdos de nivel de servicios Objetivo atractivo para ataques con motivos políticos e impactos elevados Ausencia de normativa legal local que regule la prestación de servicios en la Nube Proveedores no certificados en estándares de Seguridad de la Información. Mercado inmaduro y no posesionado a nivel gubernamental. Modificación no autorizada de información. Pérdida o fuga de información Suplantación de identidad o burla sobre los sistemas de identificación. Acceso no autorizado al sistema e información.
Vulnerabilidades	Auditoría o certificación no disponible para los clientes Ausencia de aislamiento de los recursos. Ausencia de conciencia de seguridad Ausencia de políticas de limitación de recursos Cláusulas SLA con compromisos en conflicto para con diferentes partes. Debilidades en sincronización de responsabilidades y acuerdos de nivel de servicio Falta de control en el proceso de evaluación de vulnerabilidad Falta de integridad y transparencia en los términos de uso Funciones y responsabilidades confusas Sincronización de las responsabilidades o las obligaciones contractuales externas a la nube Sistemas de certificación no adaptados a las infraestructuras de nube
Activos Afectados	Renombre de la ANT. Disponibilidad del Sistema Recaudo. Perdida de datos sensibles. Confianza del cliente Control de acceso, autenticación y/o autorización.
Controles	Proporcionar autenticación fuerte y control de acceso para el acceso de administración
Recomendaciones	Entender los distintos tipos de leyes y regulaciones y su impacto potencial en los entornos de Nube. Adecuar los acuerdos de nivel de servicio para controlar el parcheado y la corrección de vulnerabilidades Proteger el tránsito de datos mediante el cifrado de los mismos
Riesgos	Alto

Tabla 3.2.3.1.10: Evaluación riesgos de jurídicos o legales.

- ***R23: Riesgos de la Protección de Datos***.- Actualmente las infraestructuras de proveedores de Nube almacenan grandes cantidades de datos, siendo el Sistema de Recaudación de la Agencia Nacional de Tránsito uno más de esos datos. El tratamiento de los datos es uno de los elementos más complicados pues se debe garantizar por un lado la disponibilidad e integridad de la información y por otro el correcto uso de la misma, evitando así ataques de acceso, robo de información o la utilización indebida.

  Desde la perspectiva de la Agencia Nacional de Tránsito debe estar claro que será el principal responsable del procesamiento del Sistema Recaudo, incluso cuando dicho procesamiento lo realice el proveedor de Nube en su calidad de procesador externo, por lo tanto deberá implementar medidas de mitigación para la protección de la información.

Probabilidad	**Alta**
Impacto	Alto
Amenazas	Sistema débil de autenticación y autorización. Acceso remoto débil a la interfaz de administración o gestión. Espionaje de información sobre datos transmitidos o almacenados Modificación no autorizada de información. Mal funcionamiento o denegación del servicio. Problemas derivados de las tecnologías compartidas Interfaces y API poco seguros Abuso y mal uso del cloud computing. Proveedores no certificados en estándares de Seguridad de la Información.
Vulnerabilidades	Falta de control en el proceso de evaluación de vulnerabilidad. Falta de aislamiento en los recursos del cliente. Débil cifrado en el almacenamiento y trasmisión de datos. Vulnerabilidades del hipervisor Modelado inadecuado del uso de recursos. Vulnerabilidades del sistema o del sistema operativo Recursos de filtrado inadecuados o mal configurados Ausencia de conciencia de seguridad Responsabilidad por pérdida de datos
Activos Afectados	Renombre de la ANT. Disponibilidad del Sistema Recaudo. Perdida de datos sensibles. Confianza del cliente
Controles	Asegurar las salvaguardas necesarias que garanticen la autenticación, la autorización y las funciones de control de acceso. Aplicar técnicas de autenticación de doble factor siempre que sea posible.
Recomendaciones	Eliminar aquellos datos considerados sensibles para la ANT, incluyendo las copias de seguridad y datos residuales de finalización.

	Proporcionar autenticación fuerte y control de acceso para el acceso de administración.
Riesgos	Alto

Tabla 3.2.3.1.11: Evaluación riesgos de protección de datos.

- **RIESGOS NO ESPECÍFICOS DE LA NUBE**

  - ***R26: Gestión de Red***.- Adicional a los riesgos específicos de la Nube, es necesario evaluar detenidamente aquellos que no lo son, a fin de abarcar todo el espectro de gestión de riesgos, uno de esos y con un alto nivel de riesgos es la Gestión de Red al que contribuye la infraestructura de la Computación en la Nube, pues al tratarse de una plataforma distribuida aumentan los puntos de fallo, siendo más difícil realizar un correcto aseguramiento, más aún, si en la propuesta no se contempla procedimientos de recuperación de desastres que definan correctamente los tiempos y puntos de recuperación.

    Por lo tanto, la materialización de este riesgo podría causar pérdidas cuantiosas a la Agencia Nacional de Tránsito, ya que la disponibilidad del Sistema Recaudo es altamente crítico y no se puede interrumpir sus operaciones.

Probabilidad	**Alta**
Impacto	Alto
Amenazas	Mal funcionamiento o denegación de servicios. Aprovechar errores en contratos o acuerdos de nivel de servicio. Ingeniería Social a empleados del proveedor. Eliminación de información sensible. Problemas derivados de las tecnologías compartidas Interfaces y API poco seguros Proveedores no certificados en estándares de Seguridad de la Información.
Vulnerabilidades	Limitación a tecnologías dadas por el proveedor Fallas de red interna (proveedor) o externa (Internet) Falta de certificación en procedimientos y normas internacionales. Ausencia o deficiencia en proceso de recuperación. Vulnerabilidades del sistema o del sistema operativo Ausencia de aislamiento de los recursos Software que no es de confianza
Activos Afectados	Renombre de la ANT. Disponibilidad del Sistema Recaudo. Confianza del cliente
Controles	Entender y negociar los contratos de los proveedores así como los procedimientos para la respuesta a incidentes requeridos por la organización.

	Asegurarse que durante una interrupción prolongada del servicio, las operaciones críticas se pueden reanudar inmediatamente y todo el resto de operaciones, en un tiempo prudente. Comprender las tecnologías que sustentan la infraestructura del proveedor para comprender las implicaciones de privacidad y seguridad de los controles técnicos.
Recomendaciones	Entender y negociar los procedimientos de respuesta a incidentes antes de firmar. Analizar los problemas de seguridad de las interfaces de los proveedores de servicio Asegurarse que la autenticación y los controles de acceso se implementan teniendo en cuenta el cifrado de los datos Monitorizar los entornos para detectar cambios no deseados en las configuraciones o la actividad Proporcionar autenticación fuerte y control de acceso para el acceso de administración Adecuar los acuerdos de nivel de servicio para controlar el parcheado y la corrección de vulnerabilidades
Riesgos	Alto

Tabla 3.2.3.1.12: Evaluación riesgos de gestión de red.

3.2.3.2 Tratar los riesgos, definir e implementar los planes de mitigación.-

Toda vez que se ha identificado y evaluado aquellos riegos cuya probabilidad de incidente frente al impacto es alta para la puesta en marcha de la contingencia del "Sistema Integrado de Recaudación del Transporte Público Urbano de los cantones de Santa Elena, la Libertad y Salinas" en la Nube, es necesario proponer medidas correctivas orientadas a mitigarlos o eliminarlos. De acuerdo al esquema de la Figura 3.2.3.1, este proceso de mitigación debe ser iterativo con el fin de determinar su tolerabilidad frente a los criterios establecidos por la alta directiva (riesgo residual), sin embargo, como alcance de la aplicación del modelo propuesto solo se contempla esta primera iteración, siendo responsabilidad de la entidad caso de estudio, realizar las iteraciones necesarias hasta alcanzar un nivel de riesgo aceptable.

Considerando que en el país el tema de la Computación en la Nube es relativamente nuevo y que hasta la presente no existen iniciativas locales orientadas a mitigar los potenciales riesgos relacionados con los servicios de Nube, en la Tabla 3.2.3.2.1, se propone un conjunto de medidas de mitigación de riesgos acopladas de la matriz de controles de la Cloud Security Alliance, previamente analizadas en el numeral 2.3, mismas que guardan relación con el sistema de

gestión de seguridad de la información y normativas usadas por la Agencia Nacional de Tránsito.

VINCULACIÓN	• Comprender las tecnologías que sustentan la infraestructura del proveedor para comprender y mitigar las implicaciones de dependencia, privacidad y seguridad. • Determinar un segundo proveedor que cumpla con los requisitos establecidos. • Identificar los componentes y sus relaciones dentro del sistema, estableciendo para cada uno de ellos la dependencia que tiene con formatos de archivo, hardware y software. • Incorporar mecanismos en el contrato y en los acuerdos de nivel de servicios que permitan controlar los procesos y controles para la portabilidad de la data por parte del proveedor, evitando el supuesto pánico bancario. • Realizar copias de seguridad periódicas a un lugar remoto usando formatos que sean reutilizables. • Utilizar en la medida de lo posible componentes con APIs y estándares abiertos.
PERDIDA DE CONTROL Y GOBERNABILIDAD	• Analizar las implicancias legales considerando las dimensiones funcionales y contractuales. • Asegurarse que la organización mantiene la propiedad intelectual de su información, en formato original. • Cerciorarse que el contrato estipule debida diligencia en el monitoreo, mantenimiento y recuperación del sistema. • Establecer claramente las funciones y responsabilidades del cliente y proveedor dentro del contrato. • Establecer mecanismos de auditoría y herramientas para que se sigan las políticas de la organización durante el ciclo de vida. • Implantar políticas y estándares en la provisión de servicios en la Nube.
CUMPLIMIENTO	• Analizar el alcance del cumplimiento normativo y si este se verá afectada y de qué forma, al migrar a la nube. • Crear una cláusula que especifique el derecho de auditar. • Implementación de salvaguardas técnicas, físicas y administrativas, como el cifrado de los datos por parte de la ANT. • Recabar evidencia de cumplimiento para cada requisito. • Revisar que los posibles proveedores cumplan con las certificaciones y controles requeridos. • Revisar y valorar las medidas del proveedor con respecto a las necesidades de la organización.

FALLOS DE AISLAMIENTO	• Desde la perspectiva del hipervisor la Agencia Nacional de Tránsito debe entender la virtualización y otras técnicas de aislamiento que el proveedor emplee y valorar los riesgos implicados. • El proveedor de Nube debe garantizar que la información estará correctamente aislados y que los procedimientos de cifrado de la información se realizarán por personal experimentado, ya que el cifrado de los datos mal realizado también puede producir problemas con la disponibilidad de los datos o incluso la pérdida de los mismos. • Exigir mecanismos y procedimientos claros de separación para la información y control de acceso. • Realizar monitoreo sobre los procedimientos y validar sistemas de acceso e integridad de la información. • Se deben conservar los registros detallados de las actividades internas, el proveedor debe adoptar políticas de rotación de empleados y también se deben adoptar políticas de «need-to-know».
ABUSO DE FUNCIONES PRIVILEGIADAS	• Asegurar las salvaguardas necesarias para hacer seguras la autenticación, la autorización y las funciones de control de acceso. • Consensuar con el proveedor los usuarios que tendrán acceso a la infraestructura del Sistema Recaudo, para minimizar así los riesgos de que haya usuarios con elevados privilegios que no deberían tener acceso a los datos. • Definir, por contrato, el establecimiento de roles y funciones a nivel de proveedor. • Determinar los posibles problemas en los procesos de notificación. • Especificar cláusulas legales y de confidencialidad en los contratos. • Monitorizar las sesiones en busca de actividades inusuales • Prohibir, mediante políticas, compartir credenciales entre usuarios y servicios • Proporcionar autenticación fuerte y control de acceso para el acceso de administración.
PROBLEMAS JURÍDICOS Y POLÍTICOS	• Adecuar los acuerdos de nivel de servicio para controlar el parcheado y la corrección de vulnerabilidades • Asegurarse que las leyes que gobierna al proveedor de nube no entren en conflicto la normativa legal para las entidades gubernamentales. • Cada elemento (datos, aplicación y equipo) debe ser asignando un dominio para facilitar el mapeo adecuado de cumplimiento • Entender los distintos tipos de leyes y regulaciones y su impacto potencial en los entornos de Nube. • Proteger el tránsito de datos mediante el cifrado de los mismos

PROTECCIÓN DE DATOS	• Aplicar técnicas de autenticación de doble factor siempre que sea posible. • Asegurar las salvaguardas necesarias que garanticen la autenticación, la autorización y las funciones de control de acceso. • Eliminar aquellos datos considerados sensibles para la ANT, incluyendo las copias de seguridad y datos residuales de finalización. • Establecer mecanismos de redundancia de información • Generar una política para el ciudadano de la información: acceso, modificación, respaldo, eliminación, etc. • Realizar una clasificación de toda la información determinando su grado de sensibilidad frente a la integridad, confidencialidad y disponibilidad. • Utilizar mecanismos de cifrado en transmisión y almacenamiento, y tal vez a futuro en su procesamiento con la evolución de la criptografía homomófica.
GESTIÓN DE RED	• Asegurarse que durante una interrupción prolongada del servicio, las operaciones críticas se pueden reanudar inmediatamente y todo el resto de operaciones, en un tiempo prudente. • Cerciorarse que el acuerdo de nivel de servicio especifique la tasa de disponibilidad de los sistemas, tiempo y punto de restauración (RTO y RPO) y la respectiva indemnización en caso de un incidente o el no cumplimiento de lo pactado. • Comprender las tecnologías que sustentan la infraestructura del proveedor para comprender las implicaciones de privacidad y seguridad de los controles técnicos. • Desde la perspectiva de la Agencia Nacional de Transito se debe realizar un análisis del impacto del negocio (BIA), para en base a este determinas acciones que permitan mantener la continuidad de los procesos críticos. • Determina si el proveedor tiene recursos (humanos y tecnológicos) dedicados al cumplimiento del plan de continuidad. • Entender y negociar los contratos de los proveedores así como los procedimientos para la respuesta a incidentes requeridos por la organización. • Verificar que el proveedor cuente con un plan de continuidad del negocio por estándares internacionales.

Tabla 3.2.3.2.1: Medidas para mitigación de riesgos servicios de Nube Sistema Recaudo.

3.2.3.3 Aceptar el riesgo.-

La aceptación del riesgo o riesgo residual al igual que la puesta en vigencia del presente Modelo de Gestión de Riesgos es responsabilidad del directorio de la Agencia Nacional de Tránsito, mismo que deberá ser aprobado mediante resolución para cumplimiento obligatorio a todo nivel organizacional. Para lo cual se

apalancará de las recomendaciones y sugerencia del Comité de Gestión de Riesgos, quienes tienen la responsabilidad de analizar y evaluar los resultados de la implementación de los controles propuestos tanto en el numeral 2.3, como en la Tabla 3.2.3.2.1, para la puesta marcha de la contingencia del “Sistema Integrado de Recaudación del Transporte Público Urbano de los cantones de Santa Elena, la Libertad y Salinas” en la Nube.

3.2.3.4 Llevar un control de seguimiento y monitoreo del riesgo tratado.-

El monitoreo y seguimiento del riesgo es responsabilidad del Comité de Gestión de Riesgos, quienes deben garantizar que los servicios de Nube contratados, cumplen con todos los requerimientos acordados con el proveedor de servicio de Nube en materia de seguridad de la información, a través de la suscripción del Contrato y sus respectivos Acuerdos de Nivel de Servicio.

Es necesario que el Comité de Gestión de Riesgos, revise periódicamente el cumplimiento de los acuerdos de nivel de servicio y que los compare con los registros de monitoreo, ya que es imperativo garantizar la disponibilidad continua del “Sistema Integrado de Recaudación del Transporte Público Urbano de los cantones de Santa Elena, la Libertad y Salinas”, evitando la sobrecarga de las capacidades contratadas a través de la planificación de largo plazo basada en datos de monitorización. Para lo cual, se puede utilizar los controles sugeridos en el numeral 2.3 e integrarlos a los flujos de trabajo existentes, a las soluciones de la mesa de servicios, a la medición del uso, a las bases de datos de administración de configuración, etc.

3.3 ANÁLISIS DE IMPACTO Y RESULTADOS DEL MODELO

Con el desarrollo e implementación del “Modelo de Gestión de Riesgos de Infraestructura como Servicios (IaaS) de Cloud Computig para Entidades del sector público ecuatoriano”, en la Agencia Nacional de Tránsito, se ha logrado evidenciar que independientemente de las potenciales ventajas y beneficios que puede proveer la Computación en la Nube, ésta aún no está siendo explotada en su plenitud en el mercado ecuatoriano por parte de las entidades públicas, donde debido a normativas locales, no se garantizan la igualdad competitiva con la empresa privada y terminan beneficiando a proveedores del sector público, quienes aún se encuentran en proceso de implementación, construcción y fortalecimiento de sus Centros Tecnológicos Integrados bajo estándares internacionales (TIER III), y la respectiva capacitación del recurso humano en Gestión de Servicios de Nube [67], lo que da a entender, que no se encuentran en la capacidad de cubrir todo el espectro que define el término “Computación en la Nube” [10]. Por lo tanto, las amenazas y debilidades de Nube terminan por imponerse sobre sus fortalezas y oportunidades.

La puesta en marcha de las tres fases establecidas para el modelo propuesto, ha permitido diseñar un nuevo Modelo de Gestión de Riesgos de Infraestructura como Servicios (IaaS) de Cloud Computing aplicado a entidades del sector público ecuatoriano, como resultado del mapeo de normas, estándares y mejores prácticas del sector (ISO, ISACA, CSA, ENISA), el cual se esquematiza en la Figura 3.2.3.1, y que sirve como guía para una adecuada gestión de riesgos de servicios de Nube en entidades del sector público ya que abarca todo el ciclo de vida y a todo nivel organizacional.

De acuerdo a la Figura 3.2.3.1, el marco de trabajo propuesto es iterativo, ya que permite en cualquiera de sus tres fases incorporar variables no consideradas o no conocidas, garantizando la mejora continua.

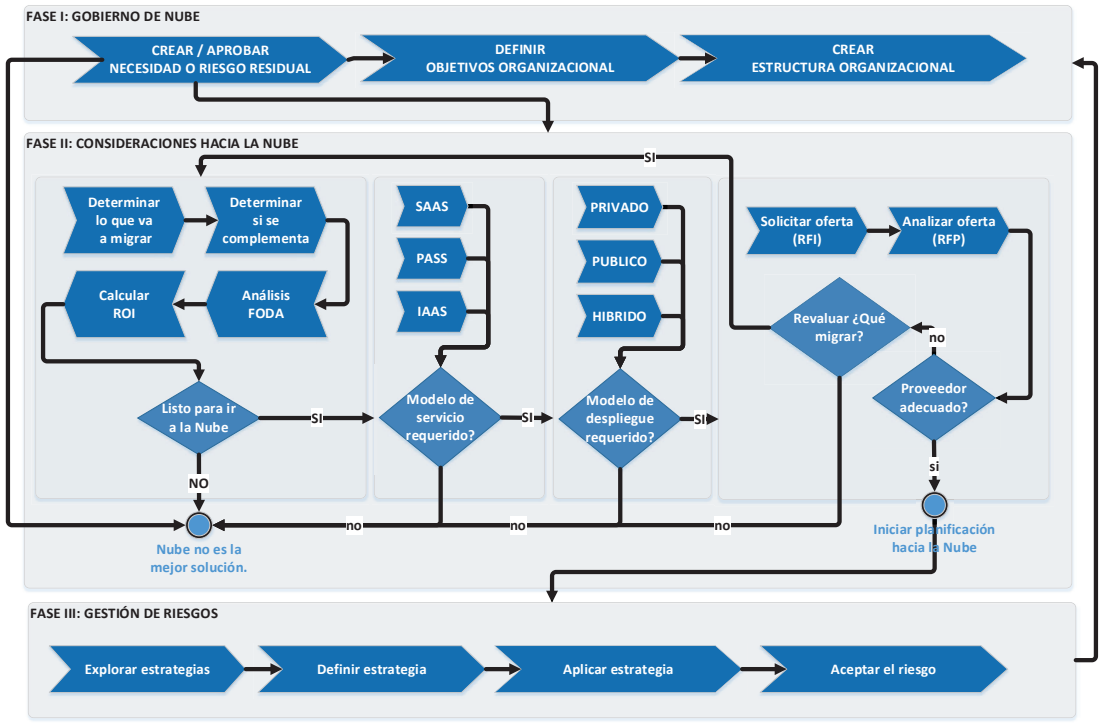

Figura 3.2.3.1 Flujo de procesos modelo de gestión de riesgos servicios de Nube.

A nivel de Gobierno de Nube, se establece, que por parte del Directorio de la Agencia Nacional de Tránsito existe la predisposición de incorporar servicios de Nube, siempre y cuando los costos de implementar contramedidas para mitigar los riesgos sean rentables para la organización (Riesgo Residual), para lo cual se establece los objetivos y la estructura organizacional que regirá todo el ciclo de vida para la gestión de riesgos de servicio de Nube.

El aporte principal del modelo propuesto se centra en la fase dos o consideraciones de Nube, misma que es el resultado de la recopilación de un sinnúmero de iniciativas internacionales y de la región por normar o regular los servicios de Nube y de proponer medidas de mitigación a los potenciales riesgos que atentan contra la seguridad, integridad, confidencialidad, privacidad y disponibilidad de la información. Mediante la implementación de esta fase se logró determinar que la computación en la Nube, por el momento, no es la mejor solución para la Agencia Nacional de Tránsito ya que los costos exceden los beneficios esperados, esto quizá por la falta de una normativa legal que regule el proceso de contratación y

provisión de servicios por parte de los proveedores de Nube, garantizando una competencia equitativa entre la empresa pública y la privada.

Para finalizar, la fase tres o de Gestión de Riesgos del modelo propuesto, permitió a la Agencia Nacional de Tránsito identificar y analizar los potenciales riegos de servicios de Nube, cuya probabilidad de incidente frente al impacto es alta. Riegos a ser mitigados mediante la puesta en marcha de un conjunto de contramedidas rentables que no exceden los beneficios esperados, en todo caso, es potestad del Directorio determinar si una contramedida es rentable y si los riesgos residuales se mantiene o deben ser mitigados, siendo necesario realizar una nueva evaluación de riesgos o concluir que la nube no es la mejor solución. Considerando el surgimiento tanto de nuevas tecnologías de servicio en la nube, como de nuevas vulnerabilidades, amenazas y contramedidas, y los cambios notorios en la legislación y/o normativa vigente. Es necesario que esta fase se complemente mediante un monitoreo y evaluación permanente por parte del Comité de Gestión de Riesgos, quienes deben comunicar dichos resultados a todo nivel organizacional en especial al directorio de la Agencia Nacional de Tránsito.

CAPITULO 4

CONCLUSIONES Y RECOMENDACIONES

En este capítulo se presentan las conclusiones y recomendaciones para el proyecto Modelo de Gestión de Riesgos de Infraestructura como Servicios (IaaS) de Cloud Computing aplicado a entidades del sector público ecuatoriano.

4.1 CONCLUSIONES

- Con la implementación del modelo de gestión de riesgos de infraestructura como servicios (IaaS) de Cloud Computing en la Agencia Nacional de Tránsito, se ha logrado determinar, que por el momento, las soluciones de Nube no es la mejor opción para garantizar la integridad, confidencialidad y disponibilidad del Sistema Integrado de Recaudación ya que los costos de implementar contramedidas para mitigar los potenciales riesgos no son rentables para la institución.
- El caso de estudio demuestra que el nivel de adopción de la computación en nube por parte de entidades gubernamentales en el territorio ecuatoriano aun es bajo, debido a las limitantes de los proveedores locales por garantizar la seguridad, la privacidad y la alta disponibilidad de la información de nube, constituyéndose en los principales obstáculos y/o factores determinantes a tenerse en cuenta a la hora de migrar u optar por los servicios de nube. Además, existe una clara necesidad de disponer de prototipos y pilotos de nube que permitan poner a prueba la utilidad y la eficacia que el modelo de negocio de la nube puede ofrecer a la administración pública.
- El estado ecuatoriano como potencial usuario de la computación en la nube debe considerar que la mejor oferta de servicios en la nube es aquella que se base en habilidades, mejores prácticas y activos desarrollados a través de años de experiencia en gestión y operación de seguridad de TI en nube, con centros de datos empresariales fiables debidamente certificados y operando bajo estándares internacionales de seguridad, que anteponga los requerimientos normativos vigentes de seguridad de TI del estado

ecuatoriano. A esto debe sumarse que la infraestructura en la que serán alojados los activos de información gubernamental deben cumplir y operar bajo las más exigentes políticas de seguridad internacionalmente aceptadas, lo que incluye procesos de análisis de seguridad regulares y acciones administrativas y operativas controladas.

- La computación en la nube ofrece a las organizaciones (pública, privada y usuario final) grandes beneficios, como pueden ser la deslocalización, la alta disponibilidad, el acceso a información desde cualquier lugar, la flexibilidad en asignación de recursos y un ahorro económico significativo, sin embargo, para entidades públicas como la Agencia Nacional de Tránsito que cuenta con el presupuesto, el recurso técnico y económico suficiente, la adopción de la nube no es la mejor solución ya que acarrea riesgos a la seguridad de la información de la ciudadanía que maneja. Se evidencia que las soluciones de nube tendrán un mayor efecto y beneficio en las Administraciones Públicas con presupuestos económicos limitados, ya que puede suponer una oportunidad para la modernización y adaptación a las nuevas tecnologías con un importante ahorro de costes y optimización de recursos de TI.
- Se prevé, que el futuro de las tecnologías de la información en las entidades de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva tendrá un carácter mixto, en el que convivirán sistemas de información propios, el housing/hosting tradicional y soluciones de Nube en cualquier de sus modalidades (públicas, privadas y/o hibridas) y tipo de servicio (IaaS, PaaS y SaaS). Debido a la falta de control físico sobre la infraestructura de nube, los acuerdos de nivel de servicio (SLA), los requisitos contractuales y la documentación del proveedor desempeñan un papel importante en la gestión de riesgos frente a la infraestructura tradicional propiedad de la organización.
- Mediante la incorporación de la computación en la nube por parte de las entidades de la Administración Pública, el gobierno ecuatoriano busca aprovechar todas las bondades que brinda este nuevo paradigma tecnológico en la provisión de servicios de TI compartidos, estandarizados,

oportunos y eficientes, mismo que se encuentra contemplado en el Plan Nacional de Gobierno en Línea, de tal manera que las instituciones gubernamentales se enfoquen en sus funciones de brindar un servicio eficiente y de calidad a la ciudadanía, sin embargo, por el momento a nivel normativo y reglamentario queda mucho trabajo por hacer.

- Pese al apoyo del estado ecuatoriano – nuevos centros de datos, penetración del internet, banda ancha, contratación por régimen especial – a proveedores de nube gubernamentales, se percibe que la industria aún se encuentra en fase de implementación de soluciones e intentando captar nuevos usuarios que le permita devengar las inversiones realizadas para garantizar la fiabilidad y calidad de sus servicios e infraestructuras en el territorio nacional.
- Buena parte del territorio ecuatoriano aún tiene velocidades promedio de acceso a Internet relativamente bajas debido a que, no ha existido un despliegue extenso de redes físicas (WAN) y las redes dorsales de fibra óptica continúan presentando limitaciones en cuanto a su despliegue, constituyéndose en un reto al que deben enfrentar los proveedores de servicios en la nube, si quieren proveer sus servicios de manera confiable y segura.
- La flexibilidad que provee la computación en la nube en comparación con la externalización tradicional de servicios de TI (correo electrónico) suele tener como contrapartida una menor seguridad para el cliente debido a que los contratos y los acuerdos de nivel de servicios que se suscribe con el proveedor de nube no son suficientemente específicos ni equilibrados y terminan favoreciendo al proveedor de nube y no a la entidad gubernamental.
- Todo elemento de desconfianza o riesgo, supone un importante freno para su implantación y para las posibilidades que la solución permite, mermando su consolidación, no siendo la excepción la computación en la nube por parte del gobierno ecuatoriano, en especial si dicha desconfianza tiene una clara connotación jurídica, que puede mitigarse a través de su correspondiente

relación contractual donde se especifique claramente deberes y responsabilidades tanto por parte del usuario como del proveedor de nube.

- A pesar de los riesgos, la adopción generalizada de la computación en nube es inevitable, ya que las organizaciones pueden lograr una agilidad real de negocios en cuanto a la TI. Sin embargo, la migración exitosa requiere de una revisión a fondo de la estructura organizacional, procesos y tecnología, así como de un entendimiento del impacto en el negocio y los riesgos que se presentan. La evaluación de riesgos de la nube puede ayudar a su organización a entender cuáles son estos riesgos antes y durante la adopción de la nube.
- Considerando las preocupaciones y riesgos que involucran las iniciativas de computación en la nube, cada entidad debe validar sus requerimientos y necesidades en base a los imperativos, la estrategia tecnológica y el apetito por el riesgo previo a emprender su vuelo hacia la nube. La metodología propuesta puede utilizarse para ayudar a decidir que aplicaciones deben estar en la nube, si es que alguna de ellas debe estar allí.
- Implantar un modelo de computación en la nube gubernamental implica trabajar previamente en la identificación de servicios comunes que se gestionan en varios organismos de la administración pública ecuatoriana de forma análoga y trabajar en la estandarización de los procesos de gestión que posibiliten que se puedan adoptar soluciones de nube globales.
- Aspectos como el impacto organizativo y adaptativo del personal, las discrepancias sobre seguridad y protección de datos, las dudas sobre rendimiento de los servicios ofertados y el efecto de cautividad por parte de proveedores de computación en la nube, se perfilan como los principales limitantes para que el estado ecuatoriano confié sus activos tecnológicos críticos, más aún si no existe normativa legal que la regule.
- La seguridad y la propiedad de los datos son aspectos claves a ser considerados a la hora de optar por una solución de computación en la nube, más aún cuando este tipo de infraestructuras pueden gestionar los datos desde múltiples países generando conflictos en cuanto al marco legal en el que son tratados, sin embargo, para el caso del estado ecuatoriano este

inconveniente es solventado mediante el acuerdo ministerial 166 de la Secretaría Nacional de la Administración Pública; acuerdo que es aprovechado por los proveedores de nube gubernamental para monopolizar el mercado e impulsar la competencia desleal frente a proveedores de nube extranjeros.

- Está claro que el retorno de la inversión (ROI) en la computación en la nube no es directo, en algunos casos los ahorros en los costos son notables, sin embargo, pueden aparecer costos inesperados que se deben tener en cuenta para calcular una estimación significativa, la cual deben incluir los costos a corto, mediano y largo plazo, los beneficios tangibles e intangibles, y el costo de mitigar cualquier riesgo nuevo que surja de la nube.
- El establecimiento de políticas de identidad y control de acceso basada en políticas de mínimo privilegio se perfilan como contramedidas esenciales en entornos de Cloud Computing, donde, por lo general la infraestructura es compartida por múltiples clientes o arrendatarios que a la postre puede provocar accesos no autorizados a información confidencial y sensible de la organización.
- Las iniciativas por estandarizar la seguridad de los servicios en la nube se fundamenta en un conjunto de procesos, políticas, métodos y mejores prácticas que buscan asegurar que los controles se realizan en un entorno adecuado para el correcto funcionamiento de la infraestructura de TI en nube, considerando aspectos relativos al acceso, identidad y manipulación de los datos, por lo que el aseguramiento de los clientes exigirá que los proveedores de nube ofrezcan un alto grado de transparencia en sus operaciones.
- Existe una frustración generalizada entre los actores de la computación en la nube, respecto al marco regulador que debería regir al mercado de nube, más aún, si dichas regulaciones son inconsistentes, contradictorias y difíciles de aplicar para los clientes y los proveedores que operan a nivel mundial, lo que frena la adopción de la computación en la nube ya que se teme que las disposiciones regulatorias nacionales no sean suficientes para garantizar la privacidad, confidencialidad y seguridad de sus datos contra accesos

indebidos por parte de organismos de control del país donde residen la información sin la debida autorización y conocimiento del cliente.

- Si bien existen divergencias en cuanto al valor que aportará la computación en la nube a la Administración Pública, sin embargo las partes interesadas entienden y visualizan los potenciales beneficios económicos y operativos de este nuevo modelo frente a la propia centralización, consolidación o externalización de servicios compartidos por múltiples organismos públicos, independientemente de que se apueste por una implementación en la nube o una solución tradicional.
- Hoy en día los aspectos de seguridad y de alta disponibilidad encabezan la lista de preocupaciones, por encima a los de la confiabilidad, telecomunicaciones y económicas, a las que debe afrontar casi la gran mayoría de potenciales clientes de nube, quienes ven en la nube la mejor opción de mejorar la calidad y niveles de servicios de su actual entorno de TI.
- Cada vez, nuevos usuarios buscan soluciones de Nube ágiles, diseñadas para proporcionar un acceso rápido a los recursos de TI en modalidad pago por uso, con las características y funciones incorporadas específicamente para satisfacer sus necesidades de TI. Soluciones que deberían incluir, entre otras cosas, pools de capacidades reservadas, funciones de administración de cuentas, compartimiento de imágenes y conectividad segura (VPN) hacia sus recursos de nube.
- La computación en la nube provee una amplia gama de productos y servicios bajo demanda para ayudar a satisfacer las diferentes necesidades de sus clientes, lo cual incluye la gestión de la seguridad y disponibilidad para proporcionar visibilidad, control y automatización, sin embargo dichas funcionalidades tienen costos adicionales, que encarecen la solución.
- Un completo beneficio de la computación en nube, exige de sus potenciales clientes que los datos, las aplicaciones y los sistemas estén asegurados adecuadamente para que la infraestructura de nube no exponga a la organización al riesgo; ya que como es de esperarse la computación en la nube viene con todos los requisitos habituales de seguridad y disponibilidad

de TI tradicional, pero con un mayor nivel de riesgo y complejidad debido a los aspectos externos; riesgos que exigen un marco global de seguridad de la información que ayude a asegurar que todos los diferentes dominios de seguridad trabajan juntos de una manera holística y sinérgica, en alineación con los principales objetivos del negocio.

- Considerando que la responsabilidad sobre los datos es del cliente, la seguridad de los mismos debe partir de éste, por lo tanto, será necesario que el potencial cliente de nube, establezca los requerimientos de seguridad de sus datos para que el proveedor de nube diseñe un servicio específico a los requerimientos de la organización.
- El sector público en su calidad de mayor comprador o potencial usuario de servicios de computación en la nube, debería poder establecer requisitos estrictos respecto a las características, prestaciones, seguridad, interoperabilidad y portabilidad de los datos, así como el cumplimiento de los requisitos técnicos conforme a la normativa local vigente, sin embargo, la realidad es muy distinta, donde las condiciones contractuales y acuerdos de nivel de servicios (SLA) del proveedor terminan por imponerse, más aún cuando el organismo que ejerce la rectoría del sistema nacional de contratación pública dentro de su normativa no prevé este tipo de contratación/servicios.
- Las normas y los modelos de riesgo han venido evolucionando de acuerdo con la forma como se administra la información en las organizaciones, brindando el conocimiento que permite tomar decisiones para disminuir costos y aumentar la rentabilidad, no siendo la excepción la computación en la nube al servicio del gobierno.
- Considerando que la innovación impulsa rápidos desarrollos de soluciones, los intermediarios de servicios en la Nube surgen como un importante componente en este nuevo ecosistema de TIC’s, al proporcionar a los usuarios y/o proveedores de servicios de Nube diversidad de métodos de interacción (APIs), lo que permite al usuario final mayor fluidez y agilidad para aprovechar el modelo que mejor se adapte a sus necesidades particulares.

- Las APIs estándar y abiertas, que tratan de habilitar aspectos como la gestión, la seguridad y la interoperabilidad en la Nube, juegan un papel clave en la portabilidad e interoperabilidad de la Nube así como en los formatos de contenedores comunes tales como el DMTF's Open Virtualization Format (OVF).
- Muchas de las barreras para la adopción de la computación en la nube son exageradas u obsoletas, más aún, cuando una solución de nube puede ser más segura y confiable que los ambientes de TI tradicionales; sin embargo, otras siguen presentando potenciales riesgos, que atentan contra la confidencialidad de la información y aplicaciones críticas del negocio.
- El mapeo de metodologías, marcos, estándares y buenas practicas existentes en el mercado, para la Gestión de Seguridad de la Información, tales como COBIT, OCTAVE e ISO, ayudan a las partes interesadas a entender cómo se interrelacionan entre sí para una adecuada gestión de riesgos de Infraestructuras como Servicios de Cloud Computing.
- Pese a que la computación en nube es considerada como el nuevo paradigma en el campo de la TIC's, no debería ser considerada como tal, sino más bien como una nueva implementación o aplicación de la tecnología existente al servicio de la sociedad que busca una economía altamente escalable y flexible, pero dentro de los estándares de seguridad de la información.
- La abstracción del hardware y la aparente pérdida del control de seguridad sobre los servicios que trae consigo la computación en la nube, da la sensación de que el nivel de seguridad es inferior al de los modelos tradicionales. Sin embargo, si las políticas de seguridad del proveedor están bien definidas, y el cliente las ejecuta fielmente, trabajar en la nube supone una mejora en la seguridad
- Dependiendo del tipo de servicio contratado, conforme se incremente el nivel de abstracción disminuye el control por parte del cliente sobre la infraestructura. Del mismo modo cuanto mayor control tiene la organización cliente sobre la infraestructura que proporciona el servicio, mayor nivel de

seguridad y control puede aplicar sobre ésta y por lo tanto sobre la información tratada.

- Los contratos de acuerdo de servicio, deben de ser revisados y creados específicamente, detallando los controles, las normativas, las medidas de protección, los plazos de recuperación del servicio, entre otros.
- Comprender el entorno actual y la relación entre la computación en la nube y los objetivos empresariales ayudan a las partes interesadas a mitigar o evitar los puntos de tensión y/o riesgos y a optimizar sus recursos de una manera más efectiva y eficiente.
- Los marcos de trabajo como COBIT han ganado fuerza como estándares de auditoría en compañías de servicios y son muy conocidos entre los proveedores de servicios en la nube. Sin embargo, carece de una serie de criterios estandarizados para los tipos de objetivos de control que puedan ser evaluados en un proveedor de servicios en la nube.
- Iniciativas por parte del gobierno ecuatoriano, está impulsando a que cada vez más entidades gubernamentales opten por la computación en la nube, como alternativa de ofrecerles importantes oportunidades en términos de escalabilidad, elasticidad, rendimiento, resiliencia y seguridad a bajo costo, lo que a su vez le permite el desarrollo de políticas públicas al servicio del ciudadano como lo son el acceso a la información, la educación y la salud.
- El uso de tecnologías de computación en la nube resulta en ahorros de costos a los presupuestos de TI (capital, personal, energía y refrigeración) de las organizaciones que, a su vez, impulsan un aumento en la rentabilidad. Sin embargo, se prevé que la adopción de esta tecnología requerirá de nuevos gastos, sobre todo si se utilizan modelos de nubes híbridas y públicas.

4.2 RECOMENDACIONES

- Es necesario que el estado ecuatoriano como miembro de la Comunidad de Estados Latinoamericanos y Caribeños (CELAC) e integrante de la Cumbre CELAC-UE, impulse el desarrollo de normas comunes a ambas regiones en lo relacionado a la computación en la nube, semejantes a las ya existentes

en la Unión Europea, una de las organizaciones internacionales más preocupada por la protección de la privacidad y la seguridad de la información que se maneja en la Computación en la Nube. Más aún, si se estima que la introducción y masificaciones de este nuevo modelo de TI impulsará la creación de pequeñas empresas y empleos en la región [69].

- Al igual que los países pioneros en la adopción de computación en la nube por parte de sus entidades gubernamentales, es necesario que el estado ecuatoriano cree una Asociación Ecuatoriana de Computación en la Nube (AECN), que agrupe a expertos y a usuarios del sector público o privado para trabajar de una manera conjunta, abierta y transparente en la elaboración de un marco de trabajo o requisitos comunes de seguridad, que deberán ser considerados durante el proceso de contratación de servicios en la nube por parte de las entidades públicas.
- Considerando que los servicios de la computación en la nube se entregan a través de las redes de telecomunicación, el Ministerio del Sector, debería impulsar iniciativas que garanticen un alto nivel de fiabilidad, disponibilidad y ancho de banda en todo el territorio nacional, lo que permitirá habilitar todo el ecosistema y el mercado de la nube en el país por parte de entidades gubernamentales.
- La existencia de mecanismos de identificación y control de acceso en los centros de datos del proveedor de nube, son algunos de los aspectos a ser considerados por el potencial usuario de Nube, a sabiendas que la administración de este tipo de infraestructura puede ser compartida por terceros y que una mala definición de las políticas puede provocar accesos no autorizados a datos confidenciales.
- Las iniciativas de adopción y/o migración de la infraestructura de TI hacia la computación en la nube deben surgir como necesidad del área de Tecnologías de la Información y no por parte de las áreas de negocio, para lo cual se sugiere comenzar con sistemas, aplicaciones y/o datos no tan críticos al Core Business de la organización y que servirán para familiarizarse con este nuevo paradigma tecnológico.

- Debido a la falta o pérdida del control físico sobre la infraestructura de TI por parte del potencial usuario de Nube, los Contratos o Acuerdos de Nivel de Servicio (SLA's), los requisitos contractuales y la documentación del proveedor desempeñan un papel muy importante en la gestión de riesgos frente a una infraestructura tradicional propietaria.
- Considerando los aspectos de flexibilidad, granularidad y multiposesión de la Computación en la Nube, las formas tradicionales de auditoría y evaluación de riesgos son modificadas o simplemente no están disponibles, debido a las políticas de seguridad de las TIC's con la que se maneja el proveedor. Quedando a criterio del potencial usuario de Nube, buscar opciones de evaluación alternativas, excepciones contractuales específicas u otro proveedor que se alínee mejor con los requisitos de gestión de riesgos institucional.
- El inventario de activos deberían incluir aquellos activos que acojan servicios en la nube y que estén bajo el control del proveedor, con planes de valoración y clasificación semejantes a los que se manejan localmente.
- Tanto, usuarios como proveedores, deberían desarrollar en conjunto escenarios de riesgo para el servicio en la nube; esto debería ser intrínseco en el diseño de servicio por parte del proveedor, y para la evaluación por parte del usuario.
- Tanto la utilización de servicios en la nube, como los modelos particulares de servicio y despliegue a ser utilizados deberían ir en concordancia con los objetivos de gestión de riesgos institucionales y con los objetivos del negocio.
- Si un proveedor de servicio en la nube no puede demostrar la existencia de procesos de gestión de riesgos exhaustivos y eficaces en relación con los servicios que presta, se debería evaluar cuidadosamente el uso de servicios en la nube en complemento con las capacidades institucionales propias, a fin de compensar posibles falencias.
- Toda organización, como potencial usuario de servicios en la nube, debe tener claro que una infraestructura de nube no solamente incluye servidores, equipos de comunicación, seguridad perimetral, dispositivos de

almacenamiento y fuentes de alimentación, sino componentes y/o salvaguardias adicionales para el control y monitoreo adecuado de su infraestructura de TI, como lo son el acceso físico a través de medidas de control de acceso biométrico y circuito cerrado de televisión (CCTV), siendo obligación del proveedor de nube explicar claramente cómo se gestionan, el acceso físico a los servidores por parte del cliente anfitrión o huésped.

- El proveedor de servicio de nube debe garantizar un modelo de aprovisionamiento rápido, fiable y seguro de recursos TI, basado en estándares, normas, mejores prácticas y productos probados en el manejo y operación de alta seguridad, con centros de datos fiables que cumplan la normativa local vigente a fin de atender los fuertes cambios en la demanda; reducir tiempos de adquisición, instalación y configuración; resolver defectos de implementación por configuraciones erróneas; sin que esto suponga incrementos en costos de gestión.
- Proporcionar la capacidad de diagnóstico a fin de determinar rápidamente la causa raíz de cuellos de botella y degradaciones en el rendimiento de infraestructura crítica en el cumplimiento de los objetivos del negocio [IBM SmartCloud Application Performance Management]
- Monitoreo del estado y el rendimiento de la infraestructura de computación en la nube público o privado, incluidos aquellos entornos que contienen tanto componentes virtualizados como físicos, a fin de modelar cambios, reducir riesgos, mejorar la disponibilidad y reducir los costes de energía y servidor. [IBM SmartCloud Monitoring]
- Permitir a las organizaciones una fácil migración hacia entornos de almacenamiento ágil basado en nube, que a su vez permita optimizar el consumo de almacenamiento, la gestión de capacidades, la supervisión de disponibilidad y la creación de informes. Funciones de copia de seguridad y restauración instantáneas a fin de proteger los datos sin afectar al rendimiento de las aplicaciones. Herramientas de administración visual simplificada que incluya interfaz de usuario avanzada basada en web. [IBM Virtual Storage Center]

- Gestor de parches de fácil administración y menor complejidad, que optimice el ciclo de actualización y que otorgue visibilidad y control sobre los sistemas operativos y aplicaciones corriendo sobre infraestructura física o virtual e independientemente del contexto, la ubicación o la conectividad. [IBM SmartCloud Patch Management]
- Cada vez, nuevos usuarios buscan soluciones de Nube ágiles, diseñadas para proporcionar un acceso rápido a los recursos de TI en modalidad pago por uso, con las características y funciones incorporadas específicamente para satisfacer sus necesidades de TI. Soluciones que deberían incluir, entre otras cosas, pools de capacidades reservadas, funciones de administración de cuentas, compartimiento de imágenes y conectividad segura (VPN) hacia sus recursos de nube.
- La Computación en la Nube está proveyendo una amplia gama tanto de productos como servicios bajo demanda para ayudar a satisfacer las diferentes necesidades de sus clientes, lo cual incluye la gestión de la seguridad y disponibilidad, mediante un probado sistema de gestión de servicios embebido para proporcionar visibilidad, control y automatización.
- Un completo beneficio de la computación en nube, exige de sus potenciales clientes, que los datos, las aplicaciones y los sistemas estén asegurados adecuadamente para que la infraestructura de nube no exponga a la organización al riesgo. Como es de esperarse la Computación en la Nube viene con todos los requisitos habituales de seguridad y disponibilidad de TI tradicional, pero con un mayor nivel de riesgo y complejidad debido a los aspectos externos. Riesgos que exigen un marco global de seguridad de la información que ayude a asegurar que todos los diferentes dominios de seguridad trabajan juntos de una manera holística y sinérgica, en alineación con los principales objetivos de negocio.
- Es necesario que los gobiernos de la región e integrantes de la CELAC impulsen el desarrollo de un marco regulatorio, que armonice los principios básicos de regulación que difieren entre jurisdicciones, a fin de mantener el ritmo de los rápidos cambios tecnológicos semejantes a los de la Unión Europea o al de Norte América. Marco con un enfoque de coregulación, en

el que la industria toma el liderazgo en la identificación de las disposiciones necesarias y los gobiernos mantengan una política y un papel de supervisión

- La computación en la nube no sólo constituye un avance tecnológico, sino que también tiene potencial para impactar positivamente en la sociedad, por lo tanto, es necesario buscar una solución en respuesta a argumentos en contra, como: la gestión de la información, puesto que gran parte de ella es confidencial o sensible y el gobierno es renuente a permitir que salga de sus fronteras. La seguridad, otro elemento de preocupación, puesto que se suele ser muy restrictivo al ocuparse de la información personal de los ciudadanos.
- En la actualidad, dada la madurez de los proveedores de servicios de nube, los riesgos son menores, sin embargo en el ámbito local aún no se cuenta con proveedores y/o expertos nacionales que apuesten por una implementación de nube gubernamental, dado que la normativa legal vigente restringe la contratación de proveedores de servicios extranjeros para el procesamiento y almacenamiento de información gubernamental.
- Ignorar la potencialidad de la nube puede suponer un error estratégico a largo plazo. La computación en la nube "democratiza" las tecnologías de la información, de lo cual los ciudadanos de los países en desarrollo serán los mayores beneficiados. El gobierno debe dar ejemplo sobre su implementación y adopción. El compromiso es de todos.

BIBLIOGRAFÍA

[1] P. Mell y T. Grance, Special Publication 800-145: The NIST Definition of Cloud Computing, Gaithersburg: National Institute of Standards and Technology, 2011.

[2] E. Martínez, «Confianza en la nube,» Prisacom, Madrid, 2014.

[3] CNT EP, «CNT EP dispondrá de dos mega centros de datos, en Quito y Guayaquil,» CNT EP, 25 marzo 2014. [En línea]. Available: http://www.cnt.gob.ec/index.php/categoria-noticias/1055-cnt-ep-dispondra-de-dos-mega-centros-de-datos-en-quito-y-guayaquil. [Último acceso: 24 junio 2014].

[4] Grupo El Comercio C.A., «Las empresas ecuatorianas se proyectan a la nube,» Lideres.ec, 17 septiembre 2012. [En línea]. Available: http://www.revistalideres.ec/informe-semanal/EMPRESAS-ECUATORIANAS-PROYECTAN_0_775722433.html?print=1. [Último acceso: 24 junio 2014].

[5] European Telecommunications Standards Institute, «ETSI.org,» [En línea]. Available: http://www.etsi.org/images/files/Events/2013/2013_CSC_Delivery_WS/CSC-Final_report-013-CSC_Final_report_v1_0_PDF_format-.PDF. [Último acceso: 27 junio 2014].

[6] LEXIS S.A., «Sistema Integrado de Legislación Ecuatoriana (eSilecPro),» LEXIS S.A., 1988. [En línea]. Available: http://www.lexis.com.ec/. [Último acceso: 03 Abril 2014].

[7] International Organization for Standardization, «ISO.org,» [En línea]. Available: http://www.iso.org/iso/catalogue_detail.htm?csnumber=43757. [Último acceso: 27 junio 2014].

[8] ISACA, Computación en la nube: Beneficios de negocio con perspectivas de seguridad, gobierno y aseguramiento, Rolling Meadows: ISACA, 2009.

[9] (CSA) Cloud Security Alliance, «Estudio del estado de la seguridad en Cloud Computing,» ISMS Forum Spain, Madrid, España, 2014.

[10] NIST, Special Publication 500-299: NIST Cloud Computing Security Reference Architecture, GAITHERSBURG: National Institute of Standards and Technology, 2013.

[11] Cisco Systems, Inc., «Informe anual de seguridad de Cisco 2013,» Cisco Systems, Inc., San José, CA (EE. UU.), 2013.

[12] Oficina de gerencia y presupuesto del Estado Libre Asociado de Puerto Rico, «Política No. TIG-017 - Tecnologías en la Nube,» ELA de Puerto Rico, Puerto Rico, 2013.

[13] HOSTCABI.NET, «W3BIN.COM,» 1 enero 2014. [En línea]. Available: http://w3bin.com/hosting_infographic. [Último acceso: 07 Diciembre 2014].

[14] Comisión Europea, «Liberar el potencial de la computación en nube en Europa,» Comisión Europea, Bruselas, 2012.

[15] ENISA, H. Thomas, L. Dimitra y L. Matina, «Good Practice Guide for securely deploying Governmental Clouds,» ENISA, Heraklion, 2013.

[16] (CET.LA) Centro de Estudios de Telecomunicaciones de América Latina, «Computación en la Nube: Desafío y opor tunidad en la sociedad conectada,» CET.LA, Montevideo, 2014.

[17] C. Melaños, «Análisis de los riesgos técnicos y legales de la seguridad en cloud computing.,» ETSIT UPM, Madrid, 2013.

[18] ISACA, «Principios rectores para la adopción y el uso de la computación en la nube,» ISACA, 2012.

[19] ENISA, «Computación en Nube: Beneficios, riesgos y recomendaciones para la seguridad de la información,» ENISA, Madrid, 2009.

[20] Business Software Alliance, «2013 BSA Global Cloud COMPUTING Scorecard,» The Software Alliance, Washington, 2013.

[21] EL UNIVERSO, «www.eluniverso.com,» 29 Diciembre 2014. [En línea]. Available: http://www.eluniverso.com/noticias/2014/12/29/nota/4387226/acceso-gmail-fue-bloqueado-china. [Último acceso: 06 Enero 2015].

[22] ALAI, «Agencia Latinoamericana de Información,» ALAI, abril 2014. [En línea]. Available: http://alainet.org/active/74128&lang=es. [Último acceso: enero 2015].

[23] J. Jara, «Guía para el análisis de factibilidad en la implantación de tecnologías de cloud computing en empresas del Ecuador,» EPN, Quito, 2014.

[24] C. Salazar, «Análisis de los riesgos técnicos y legales de la seguridad en cloud computing.,» UPM ETSIT, Madrid, 2013.

[25] W. Peres, «América Latina de la web a la computación en la nube,» CEPAL, Montevideo, 2013.

[26] ISACA, IT Control Objectives for Cloud Computing, EEUU: ISACA, 2012.

[27] IBM Security Systems, «IBM X-Force Threat Intelligence Quarterly,» IBM Corporation, Nueva York, 2014.

[28] Cloud Security Alliance, «Top Threats to Cloud Computing,» CSA, Madrid, 2010.

[29] G. Contesse, J. Soto, P. Caroca, E. Galuzzi, L. Graff, M. Sepúlveda, E. Witt, N. Vega y L. M. Marrey, «Tendencias 2014, a paso firme hacia la Tercera Plataforma,» GERENCIA, vol. XVII, nº 185, pp. 48-51, 2014.

[30] musictank, 2012. [En línea]. Available: http://www.musictank.co.uk/resources/reports/energy-report. [Último acceso: 19 12 2014].

[31] EUROPEAN COMMISSION, «Code of Conduct on Data Centres Energy Efficiency,» Ispra, 2008.

[32] Software Engineering Institute, «cert.org,» [En línea]. Available: http://www.cert.org/resilience/products-services/octave/index.cfm. [Último acceso: 30 enero 2015].

[33] C. Alberts y A. Dorofee, «OCTAVE(SM) Method Implementation Guide Version 2.0,» CERT, Massachusetts, 2001.

[34] International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC), NTE INEN-ISO/IEC 27005:2015 Tecnología de la Información - Técnicas de Seguridad - Gestión de Riesgos en la Seguridad de la Información, Quito: Instituto Ecuatoriano de Normalizacion (INEN), 2012.

[35] W. Carrera y S. García, «Diseño de un Modelo de Gestión de Riesgos de Seguridad de la Información Basado en el Acoplamiento de la Norma ISO/IEC 27005:2008 y el Método Octave,» Escuela Politécnica Nacional, Quito, 2012.

[36] ISACA, COBIT5: Un Marco de Negocio para el Gobierno y Gestión de las TI de la Empresa, EEUU: ISACA, 2012.

[37] Universidad EAFIT, «COBIT: Modelo para auditoría y control de sistemas de información,» EAFIT, Medellin, 2007.

[38] ISACA, «COBIT5 para Riesgos,» ISACA, Illinois, 2014.

[39] J. Matalobos, «Análisis de Riesgos de Seguridad de la Información,» Universidad Politécnica de Madrid, Madrid, 2009.

[40] ISO/IEC, «iso27000.es,» 2012. [En línea]. Available: www.iso27000.es. [Último acceso: 07 julio 2014].

[41] Cloud Security Alliance (CSA), «Consensus Assessments Initiative,» Cloud Security Alliance, 2015. [En línea]. Available: https://cloudsecurityalliance.org/research/cai/. [Último acceso: 20 Abril 2015].

[42] Registro Oficial, «Acuerdo Nro. 166 - Uso obligatorio de las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 para la Gestión de la Seguridad de la Información,» Quito, 2013.

[43] ENISA, «Cloud Computing: Information Assurance Framework,» European Network and Information Security Agency, Madrid, 2009.

[44] V. Álvarez y M. Valencia, «Propuesta de un modelo de gestión para un proveedor de cloud computing, destinado al mercado nacional y sudamericano.,» EPN, Quito, 2014.

[45] International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC), «NTE INEN-ISO/IEC 27000:2012 Tecnología de la Información - Técnica de Seguridad - Sistema de Gestión de Seguridad de la Información - Descripción General y Vocabulario,» Instituto Ecuatoriano de Normalización (INEN), Quito, 2012.

[46] Cloud Security Alliance (CSA), «cloudsecurityalliance.org,» CCM, 2009. [En línea]. Available: https://cloudsecurityalliance.org/research/ccm/. [Último acceso: 04 febrero 2015].

[47] Registro Oficial, 449 Constitución de la República del ECUADOR, Quito: LEXIS S.A., 2008.

[48] Registro Oficial, Suplemento 415 - Ley Orgánica Reformatoria a la Ley Orgánica de Transporte Terrestre, Tránsito y Seguridad Vial, Quito: LEXIS S.A., 2011.

[49] Registro Oficial, Suplemento 323 - Reglamento Órganico por Proceso de la Agencia Nacional de Tránsito., Quito: LEXIS S.A., 2012.

[50] Agencia Nacionl de Tránsito, «Agencia Nacional de Tránsito,» ANT, 2012. [En línea]. Available: www.ant.gob.ec. [Último acceso: 2015 julio 17].

[51] ISEC, «Plan Estratégico de Tecnologías de la Información,» ISEC, Quito, 2015.

[52] Registro Oficial, «Acuerdo Ministerial 1002 Suplemento 606 - Norma Técnica de Implementación y Operación de la Metodología y Herramienta de Gobierno por Resultados,» LEXIS S.A., Quito, 2011.

[53] Registro Oficial, «Acuerdo Ministerial 1580 Suplemento 895 Norma Técnica de Gestión de Procesos Secretaría de la Administración Pública.,» LEXIS, Quito, 2013.

[54] Registro Oficial, «Acuerdo Ministerial 718 RO 597 - Instructivo Para el Uso de Sistema Quipux en Administración Pública,» LEXIS S.A., Quito, 2011.

[55] Registro Oficial, «Acuerdo Ministerial 1062 Suplemento 467 - Norma Técnica de Interoperabilidad Gubernamental,» LEXIS S.A., Quito, 2015.

[56] Registro Oficial, «Suplemento 557 - Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos,» LEXIS S.A., Quito, 2014.

[57] SENPLADES, «Plan Nacional para el Buen Vivir 2013-2017,» Secretaría Nacional de Planificación y Desarrollo, Quito, 2013.

[58] EPN, «Guía Para el Análisis de Factibilidad en la Implantación de Tecnologías de Cloud Computing en Empresas del Ecuador,» Escuela Politecnica Nacional, Quito, 2012.

[59] ISACA, «COBIT 5 - Procesos Catalizadores,» ISACA, Illinois, 2012.

[60] INEC, «Instituto Nacional de Estadísticas y Censos,» INEC, 2014. [En línea]. Available: http://www.ecuadorencifras.gob.ec/. [Último acceso: 12 Agosto 2015].

[61] VMware, «Copyright © 2015 VMware, Inc.,» [En línea]. Available: http://www.vmware.com/es/products/converter. [Último acceso: 07 Septiembre 2015].

[62] Microsoft, «© 2015 Microsoft,» [En línea]. Available: https://technet.microsoft.com/en-us/library/jj158932.aspx. [Último acceso: 07 Septiembre 2015].

[63] ISACA, «Calcular el ROI de la nube: Desde la perspectiva del cliente,» ISACA, Rolling Meadows, 2012.

[64] Corporación Nacional de Telecomunicaciones, «CNT Implementa Sistema de Gestión de Seguridad de la Información,» CNT, 2015. [En línea]. Available: http://soy.cnt.com.ec/. [Último acceso: 20 Agosto 2015].

[65] Corporación Nacional de Telecomunicaciones, «Oferta de Servicio de Data Center Virtual (IaaS),» CNT, Quito, 2015.

[66] Corporación Nacional de Telecomunicaciones, «Cloud Computing: Acuerdos de Nivel de Servicios (SLA),» CNT, Quito, 2014.

[67] Corporación Nacional de Telecomunicaciones, «Resolución RE-CNTEP-1300001193-2015-001: Servicio de capacitación en ITIL Foundation y Cloud Essentials,» CNT, Quito, 2015.

[68] CEPAL, «Banda ancha en América Latina: más allá de la conectividad,» Francisca Lira, Santiago de Chile, 2013.

[69] CELAC, «La Unión Europea y América Latina y el Caribe ante la nueva coyuntura económica y social,» CELAC, Santiago, 2015.

[70] I. M. Proaño, «Cloud Computing / Computación en nube,» Universidad Politécnica Salesiana del Ecuador, Quito, 2011.

[71] P. M. I. PMI, Guía de los Fundamentos para la Dirección de Proyectos (Guía del PMBOK), Cuarta ed., Newtown Square, Pennsylvania: Global STANDARD, 2009, p. 393.

[72] E. Piraino, «Asegurando la Brecha,» GERENCIA, p. 40, 2014.

[73] R. S. Patricia Prandini, «Re-evolucion COBIT5,» ISACA Argentina, Buenos Aires, 2012.

[74] G. A. Marañon, Seguridad informática para empresas y particulares., España: McGraw-Hill España, 2004.

[75] P. Kulevicius, «"CYBERNOMICS" La seguridad cibernética hoy,» GERENCIA, pp. 44-45, 2014.

[76] W. Hálaby, «ISO 27001:2013,» (ISC) Capitulo Colombia Board Member, Colombia, 2013.

[77] N. Giannetti, «Business Intelligence en la nube,» GERENCIA, vol. XVII, nº 185, p. 46, 2014.

[78] A. D. Christopher Alberts, Managing Information Security Risks: The OCTAVE (SM) Approach, Addison-Wesley Professional, 2003.

[79] Anonymous, «Gemalto lanza solución de autenticación segura para proveedores de servicios en nube,» Business Wire, San Francisco, EEUU, 2013.

[80] Red Hat®, «Red Hat®,» 27 Agosto 2012. [En línea]. Available: www.redhat.com. [Último acceso: 3 Marzo 2014].

[81] Grupo El Comercio C.A., «La transición a la nube genera beneficios e inquietudes,» Revista Lideres.ec, 17 septiembre 2012. [En línea]. Available: http://www.revistalideres.ec/informe-semanal/transicion-nube-genera-beneficios-inquietudes_0_775722422.html. [Último acceso: 26 junio 2014].

[82] IBM CORPORATION, «Disipando el vapor en torno a cloud computing,» © Copyright IBM Corporation 2010, New York, 2010.

[83] W. Jansen y T. Grance, «Guidelines on Security and Privacy in Public Cloud Computing,» NIST, Gaithersburg , 2011.

[84] Ministerio de Hacienda y Administraciones Públicas, «Magerit versión 3.0: Metodología de Análisis y Gestión de Riesgos,» [En línea]. Available: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae

_Metodolog/pae_Magerit.html#.VMpiyC7aRfc. [Último acceso: 29 anero 2015].

[85] G. Vanegas, «Armonización de Múltiples Modelos para el Análisis de Riesgos de las Tecnologías de la Información y Desarrollo de Software,» Universidad de San Buenaventura Cali, Cali, 2013.

[86] Registro Oficial, Suplemento 337 - Ley Orgánica de Transperencia y Acceso a la Información Pública., Quito: LEXIS S.A., 2004.

[87] J. Joyanes Aguilar, «Computación en la Nube: Notas para una estratégia Española en Cloud Computing.,» Instituto Español de Estudios Estratégicos, Salamanca, 2012.

[88] CEPAL, «La nueva revolución digital,» CEPAL, Santiago, 2015.

[89] VMware, «The VMware Transformation Journey,» VMWARE, 2015. [En línea]. Available: http://www.vmware.com/products/vsphere/features/drs-dpm. [Último acceso: 01 09 2015].

[90] EMC Consulting, Creación de una nube confiable: Estrategias de implementación para nubes privadas e híbridas, Buenos Aires: EMC, 2012.

[91] Registro Oficial, Suplemento 105 - Reglamento de Recaudo para Transporte Público Intra-Cantonal, Quito: LEXIS S.A., 2014.

[92] C. Alba, «Planeación de la Seguridad de la Información Corporativa Sensible Contra Amenazas Internar,» SEPI ESIME CULHUACAN, Mexido, DF, 2011.

[93] P. Chicaiza y a. Díaz, «Diseño de un plan de gestión de seguridades de la información para instituciones públicas ecuatorianas,» EPN, Quito, 2014.

GLOSARIO

TÉRMINOS

Accesibilidad	Capacidad del Proveedor de Nube para permitir al cliente el acceso a su información con independencia de donde se almacene y a través de una multitud de dispositivos, limitada únicamente por el acceso a Internet.
Activo	El objetivo de la protección en un análisis de seguridad
Acuerdo de Nivel de Servicio	Acuerdo que especifica y garantiza las condiciones y niveles de calidad de prestación de un servicio. Se utiliza para compartir e intercambiar datos e información electrónicos entre entidades públicas proveedoras y entidades públicas consumidoras, a través de la Plataforma de Interoperabilidad Gubernamental.
Arquitectura Orientada a Servicios	Arquitectura de software que define la utilización de programas de software, acoplados y reutilizables para satisfacer los requerimientos de un sistema.
Back Offices	Conjunto de actividades de apoyo al negocio. Generalmente son labores informáticas y de comunicaciones, de gestión de recursos humanos, contabilidad o finanzas.
Cifrado	Proceso mediante el cual se toma un mensaje en claro, se le aplica una función matemática, y se obtiene un mensaje codificado.
Comercio electrónico	Es toda transacción comercial realizada en parte o en su totalidad, a través de redes electrónicas de información.

Comisión para la Seguridad Informática y de las Tecnologías de la Información y Comunicación	Creada mediante Acuerdos Ministeriales No. 804 y 837 del 2011, para el establecimiento de lineamientos de seguridad informática, protección de infraestructura computacional y todo lo relacionado con ésta, incluyendo la información contenida para las entidades de la Administración Pública Central e Institucional. Se encuentra conformada por delegados del Ministerio de Telecomunicaciones y de la Sociedad de la Información, la Secretaría Nacional de Inteligencia y la Secretaría Nacional de la Administración Pública
Community Cloud	In a Community cloud, the cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.
Conexión Remota	Operación realizada en una computadora remota a través de una red de computadoras, como si se tratase de una conexión local.
Confidencialidad	Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso (ISO 17799)
Control de acceso	Limitar el acceso a objetos de acuerdo a los permisos de acceso del sujeto.
Controlador de datos	La persona física o jurídica, autoridad pública, agencia o cualquier otro organismo que, de manera individual o conjunta, determina los fines y medios del procesamiento de los datos personales; cuando los fines y medios del procesamiento están determinados por la ley o la normativa nacional o comunitaria, el controlador o los criterios específicos para su designación pueden

	estar determinados por la legislación nacional o comunitaria.
Co-residencia	Recursos de hardware o software compartidos por clientes en nube
Cortafuegos	Herramienta de seguridad que proporciona un límite entre redes de distinta confianza o nivel de seguridad mediante el uso de políticas de control de acceso de nivel de red.
Data center	Se denomina centro de procesamiento de datos a aquella ubicación donde se concentran los recursos necesarios para el procesamiento de la información de una organización.
Depósito (Escrow)	Almacenamiento de un recurso por un tercero que puede acceder a dicho recurso cuando se cumplen determinadas condiciones bien definidas
Desaprovisionamiento	Proceso de obligar a retirar un recurso de su uso o prohibir que un conjunto de usuarios haga uso del mismo
Dimensión Contractual	Implica las estructuras, términos y condiciones de contratos y los mecanismos de aplicación a través de los cuales los grupos de interés en los entornos de cloud computing pueden afrontar y gestionar las cuestiones legales y de seguridad.
Dimensión Funcional	Implica determinar cuáles de las funciones y servicios que se producen en la Nube crean implicaciones legales para los participantes y los grupos de interés.
Dimensión Jurisdiccional	Implica la forma en que los gobiernos administran las leyes y las normativas que afectan a los servicios de Nube, los grupos de interés y los activos de datos implicados.

Disponibilidad	El porcentaje de tiempo durante el cual un sistema puede funcionar
DoS or DDoS	Denial of Service or Distributed Denial of Service attack. This type of attack can jeopardize the cloud service by saturating the limited network bandwidth and interrupting the configuration/routing information. It can also cause the computing platform to slow down responses to legitimate requests because it is overloaded with non-legitimate traffic.
EDoS	Denegación económica de servicio
Escaneado de puertos	Sondeo de un alojamiento en red para determinar los puertos que están abiertos y los servicios que ofrecen
Esquema Gubernamental de Seguridad de la Información	establece un conjunto de directrices prioritarias para Gestión de la Seguridad de la Información e inicia un proceso de mejora continua en las instituciones de la Administración Pública
Factura electrónica	Conjunto de registros lógicos archivados en soportes susceptibles de ser leídos por equipos electrónicos de procesamiento de datos que documentan la transferencia de bienes y servicios, cumpliendo los requisitos exigidos por las Leyes Tributarias, Mercantiles y más normas y reglamentos vigentes.
Firmas Electrónicas	Según la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, son los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, y que puedan ser utilizados para identificar al titular de la firma en relación con el mensaje de datos, e indicar que el titular de la firma aprueba y reconoce la información contenida en el mensaje de datos.

Gobierno por Resultados	Es una solución integral de metodologías, herramientas digitales, aprendizaje práctico y adopción de cambio para soluciones sostenibles y autosuficiencia del cliente. Busca dar transparencia y continuidad a la gestión de todas las instituciones del Gobierno Central del Ecuador mediante la definición, alineación, seguimiento y actualización de planes estratégicos y operativos en todos los niveles institucionales.
Hosting	Consiste básicamente en vender o alquilar el espacio físico donde se va a almacenar los archivos que conforman su web, sus correos electrónicos y demás información.
Housing	Consiste básicamente en vender o alquilar un espacio físico de un centro de datos para que el cliente coloque ahí su propia infraestructura.
Hypervisor	One of many hardware virtualization techniques allowing multiple operating systems to run concurrently on a host computer.
IaaS	Infraestructura como servicio. El proveedor ofrece recursos como capacidad de procesamiento, de almacenamiento o comunicaciones, que el usuario puede utilizar para ejecutar cualquier software; desde sistemas operativos hasta aplicaciones.
IaaS	In an IaaS deployment, the capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications

Integridad	Propiedad de los datos que no han sido alterados accidental o maliciosamente durante el almacenamiento o la transmisión
Interoperabilidad Tecnológica	Implementar programas de software e infraestructura tecnológica comunes para intercambiar de forma estándar y segura datos e información electrónicos entre sistemas gubernamentales.
Intimidad	El derecho a la intimidad previsto en la Constitución Política de la República, para efectos de la Ley de Comercio Electrónico, Firmas y Mensajes de Datos - LCEFMD -, comprende también el derecho a la privacidad, a la confidencialidad, a la reserva, al secreto sobre los datos proporcionados en cualquier relación con terceros, a la no divulgación de los datos personales y a no recibir información o mensajes no solicitados.
Localización	El punto geográfico concreto en el que se encuentran los datos o se realiza el proceso en un servicio de cloud computing.
Logs	Uno o más ficheros de texto automáticamente creados y administrados por un servidor, en donde se almacena toda la actividad que se hace sobre éste.
Mensaje de datos	Es toda información creada, generada, procesada, enviada, recibida, comunicada o archivada por medios electrónicos, que puede ser intercambiada por cualquier medio. Serán considerados como mensajes de datos, sin que esta enumeración limite su definición, los siguientes documentos electrónicos, registros electrónicos, correo electrónico, servicios web, telegrama, télex, fax e intercambio electrónico de datos.
No repudio	La propiedad por la que una parte del conflicto no puede repudiar o refutar la validez de una declaración o contrato

Nube híbrida	Resultado de la combinación de dos o más nubes individuales que pueden ser privadas, compartidas o públicas. Permite enviar datos o aplicaciones entre ellas.
Nube privada	Los servicios no son ofrecidos al público en general. La infraestructura es íntegramente gestionada por una organización.
Nube pública	La infraestructura es operada por un proveedor que ofrece servicios al público en general.
Objetivo de seguridad	Documento que especifica los criterios de evaluación de la seguridad para sustanciar las reclamaciones de los distribuidores relativas a las propiedades de seguridad de un producto (término utilizado en Criterios comunes)
Offshoring	O deslocalización, es el proceso por el que los bienes o servicios proceden de una filial de la propia empresa, localizada en un país distinto al de la empresa original. En definitiva existe una operación en el exterior, que pertenece a la misma empresa, lo cual le da un mayor nivel de control
Operadora de Transporte	Alusión a cooperativas y/o compañías de transporte terrestre.
Orden judicial	En este contexto, la autoridad legal que confisca las pruebas
PaaS	Plataforma como servicio. Al usuario se le permite desplegar aplicaciones propias (adquiridas o desarrolladas por el propio usuario) en la infraestructura de la nube de su proveedor, que ofrece la plataforma de desarrollo y las herramientas de programación. En este caso, el usuario mantiene el control de la aplicación, aunque no de toda la infraestructura subyacente.

PaaS	In a PaaS deployment, the capability provided to the Consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming, libraries, services, and tools supported by the Provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
Perfil de protección	Documento que especifica los criterios de evaluación de la seguridad para sustanciar las reclamaciones de los distribuidores de una familia de productos de sistemas de información concreta (término utilizado en Criterios comunes)
Perimetrización	Control del acceso a un activo o grupo de activos
Plataforma Tecnológica de Interoperabilidad Gubernamental	Sistema computacional constituido por componentes de hardware, software y redes de datos que permite intercambiar datos entre sistemas gubernamentales, de forma estándar, segura y confiable.
Política de seguridad	1. Conjunto de estatutos que describen la filosofía de una organización respecto a la protección de su información y sistemas informáticos. 2. Conjunto de reglas que ponen en práctica los requisitos de seguridad del sistema.
Portabilidad	Que los datos de un contratista que están en los servidores del proveedor de cloud puedan trasladarse a otro proveedor (o a sistemas locales) a elección del contratista y sin pérdida de datos ni de servicio.
Private Cloud	In a Private cloud, the cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be

	owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
Procesador de datos	Una persona física o jurídica, autoridad pública, agencia o cualquier otro organismo que procesa datos personales en nombre del controlador.
Productividad	Capacidad del Proveedor de Nube para permitir al cliente centrarse en temas relevantes para el crecimiento y la mejora de sus negocios, ya que actividades rutinarias de TI y de mantenimiento de red lo realiza el proveedor.
Proveedor de servicios de plataformas de la nube	Proporcionan plataformas basadas en la nube, hospedados en entornos de sistemas e infraestructuras específicos, para que los desarrolladores puedan acceder a la plataforma, desarrollar una nueva aplicación de negocios y alojarlas en la plataforma basada en la nube.
Proveedores de soluciones	Desarrollan aplicaciones o suites completas, para conseguir un amplio mercado de consumidores de la nube (otras operadoras de telefonía e internet)
Proveedores de tecnologías	Desarrollan las herramientas y tecnologías que facilitan que la nube se establezca y se proporcione a los consumidores de recursos proporcionados por la nube. Ofrecen un amplio rango de herramientas, tecnologías, sistemas operativos para facilitar el despliegue de nubes públicas, privadas, híbridas y comunitarias.
Public Cloud	In a Public cloud, the cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Red de proximidad	En este contexto, una red de ordenadores que puede procesar y almacenar dato para ser entregados cerca del destino final
Red privada virtual	Es una tecnología de red que permite una extensión segura de la red local sobre una red pública o no controlada como Internet.
Resiliencia	La capacidad de un sistema para proporcionar y mantener un nivel aceptable de servicio ante fallos (no intencionados, intencionados o derivados de causas naturales)
Resistencia/resilience	Es la capacidad de un sistema (red, servicio, infraestructura, etc.) de ofrecer y mantener un nivel de servicio aceptable frente a diversos fallos y desafíos al funcionamiento normal.
Roadmap	U hoja de ruta, utilizado para dar a conocer el "trazado del camino" por medio del cual llegar del estado actual al estado futuro. Es decir, la secuencia de actividades o camino de evolución que llevará al estado futuro.
RPO	Se refiere al volumen de datos en riesgo de pérdida que la organización considera tolerable. Determina el objetivo de posible pérdida máxima de datos introducidos desde el último backup, hasta la caída del sistema, y no depende del tiempo de recuperación. Tiempo máximo establecido entre una copia de seguridad y otra con el fin de mantener la continuidad de los servicios.
RTO	Expresa el tiempo durante el cual una organización pueda tolerar la falta de funcionamiento de sus aplicaciones y la caída de nivel de servicio asociada, sin afectar a la continuidad del negocio.

SaaS	Software como servicio. Al usuario se le ofrece la capacidad de que las aplicaciones suministradas se desenvuelvan en una infraestructura de la nube, siendo las aplicaciones accesibles a través de un navegador web, como en el correo electrónico Web. Posiblemente, este es el ejemplo más representativo, por lo extendido, de este modelo de servicio. El usuario carece de cualquier control sobre la infraestructura o sobre las propias aplicaciones, excepción hecha delas posibles configuraciones de usuario o personalizaciones que se le permitan.
SaaS	In a SaaS deployment, the capability provided to the Consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The Consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
Seguridad	Es la capacidad de proteger la información y sistemas de información frente a accesos, uso, divulgaciones, interrupciones, modificaciones o destrucciones no autorizados, así como de responder y recuperarse en caso de fallo o incidencia (12).
Sellado de tiempo	Anotación electrónica firmada electrónicamente y agregada a un mensaje de datos en la que conste como mínimo la fecha, la hora y la identidad de la persona que efectúa la anotación.

Simplicidad	Capacidad del proveedor de Nube para manejar la complejidad técnica relacionada con establecer, operar, y mantener cualquier parte del proceso de las TIC, permitiendo al cliente centrarse en su negocio.
Sistema de información	Es todo dispositivo físico o lógico utilizado para crear, generar, enviar, recibir, procesar, comunicar o almacenar, de cualquier forma, mensajes de datos.
Sistema de prevención de intrusiones	Sistema que combina las capacidades de bloqueo de un cortafuego y las de análisis de un IDS. Está diseñado para detener ataques antes de que tengan éxito.
Sistema responsable de la entrega de servicios en nube	Sistema responsable de la entrega de servicios en nube
Sistemas Gubernamentales	Programas de software de misión específica o general a partir de los cuales se desarrollan servicios para compartir e intercambiar datos con otros sistemas gubernamentales.
SSL	Capa de conexión segura (utilizada para codificar el tráfico entre navegadores y servidores web)
Sujeto de los datos	Persona física identificada o identificable (véase la Directiva UE 95/46/CE) de quien se recogen los datos y/o sobre quien se procesan los datos
TLS	Seguridad de la Capa de transporte (utilizada para codificar el tráfico entre navegadores y servidores web)
Vulnerabilidad	Cualquier circunstancia o evento que puede repercutir de manera negativa sobre un activo
Vulnerabilidades	Debilidades en un sistema que pueden ser utilizadas para violar las políticas de seguridad.

Zona desmilitarizada	Máquina o pequeña subred situada entre una red interna de confianza (como una red local privada) y una red externa no confiable (como Internet). Normalmente en esta zona se sitúan los dispositivos accesibles desde Internet, como servidores Web, FTP, SMTP o DNS, evitando la necesidad de acceso desde el exterior a la red privada. Este término es de origen militar, y se utiliza para definir un área situada entre dos enemigos.

ACRÓNIMOS

AAA	Autenticación, autorización y contabilización
AC	Autoridad de certificación
ANT	Agencia Nacional de Tránsito
API	Interfaz de programación de aplicaciones, del inglés, Application Programming Interface
CAIQ	Del inglés Consensus Assessments Initiative Questionnaire
CCM	Cloud Controls Matrix
CELAC	Comunidad de Estados Latinoamericanos y Caribeños
CEO	Chief Executive Officer
CEPAL	Comisión Económica para América Latina y el Caribe
CIO	Chief Information Officer
CISO	Oficial o Director de Seguridad de la Información, del inglés Chief Information Security Officer
CNT	Corporación Nacional de Telecomunicaciones
COBIT	Control Objectives for Information and Related Technology
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CPU	Unidad central de proceso del inglés, Central Process Unit
CRM	Customer Relationship Management
CSA	Cloud Security Alliance
CSI	Comité de Gestión de la Seguridad de la Información
CSO	Oficial de Seguridad de la Información

CSP	Cloud Service Provider
DDoS	Distribución de denegación de servicio
DMZ	Zona desmilitarizada
EGSI	Sistema Gubernamental de Seguridad de la Información
ENISA	Agencia Europea de Seguridad de Redes e Información
ERM	Gestión Integral de Riesgos del inglés Enterprise Risk Management
ERP	Enterprise Resource Planning
GAD	Gobiernos Autónomos Descentralizados
GPR	Gobierno por Resultados
GPU	Unidad de procesamiento de gráficos, del inglés Graphics Process Unit.
IAAS	Infraestructura como servicio o SaaS, del inglés Infrastructure as a Service
IAM	Administración de Identificación y Acceso, del inglés Identity Access Management
IBM	International Business Machines Corporation
IdP	Identity Provider
IDS	Sistema de detección de intrusos
IEEE	Institute of Electrical and Electronics Engineers
IPS	Sistema de prevención de intrusos
ISO	Organización Internacional de Normalización
ISP	Proveedor de Servicios de Internet, Internet Service Providers
LAN	Red de Área Local
LDAP	Protocolo ligero de acceso a directorios
LOSNCP	Ley Orgánica del Sistema Nacional de Contratación Pública
LOTAIP	Ley Orgánica de Transparencia y Acceso a la Información Pública
LOTTTSV	Ley Orgánica de Transporte Terrestre Tránsito y Seguridad Vial
MPLS	Multiprotocol Label Switching
NIS	Seguridad de las redes y de la información
NIST	Instituto Nacional de Estándares y Tecnologías (Estados Unidos) de inglés, National Institute of Standards and Technologies
OCTAVE	Operationally Critical Threat, Asset and Vulnerability Evaluation

OLA	Acuerdo de Nivel de Operación, del inglés Operating Level Agreement
OTP	Contraseña de un solo uso (tipo de símbolo de autenticación)
OVF	Formato abierto de virtualización
PAAS	Plataforma como servicio o SaaS, del inglés Platform as a Service
PRTG	Paessler Router Traffic Grapher
QOS	Calidad De Servicio
QoS	Quality of Service
ROI	Retorno sobre la inversión
ROSI	Retorno sobre la inversión de seguridad
RPO	Objetivo de Punto de recuperación
RTO	Punto de Recuperación Objetivo, del inglés Recovery Point Objective
RTO	Objetivo de Tiempo de recuperación
SAAS	Software como Servicio o SaaS, del inglés Software as a Service
SGE	Subsecretaría de Gobierno Electrónico de la SNAP
SLA/ANS	Acuerdo de nivel de servicio, del inglés Service Level Agreement
SLAP	Acuerdo de Nivel de Servicio de proveedor, del inglés Service Provider Licence Agreement
SNAP	Secretaría Nacional de la Administración Pública
SO	Sistema operativo
SOA	Arquitectura Orientada a Servicios, del inglés Service Oriented Architecture
SOAP	Simple Object Access Protocol
TCO	Total Cost of Ownership
UE-CELAC	Cumbre de la Comunidad de Estados Latinoamericanos y Caribeños y la Unión Europea
UPS	Sistema de alimentación ininterrumpida
VM	Máquina virtual
VPN	Red Privada Virtual.
XML	Extensible Markup Language

ANEXOS

ANEXO 1: ROLES, FUNCIONES, PERSPECTIVAS E IMPLICANCIAS

ALTA DIRECTIVA:

- Identifique las brechas organizacionales (en el desempeño, competitivas, geográficas, etc.) y determine si la nube le puede ayudar a cerrar esas brechas.
- Evalúe la necesidad de colaborar e intercambiar información con los proveedores y usuarios. ¿Hay elementos organizacionales donde se intercambie información que se pudiera migrar al entorno de nube? ¿Podrían estos convertirse en nuevas oportunidades de negocio y en maneras de ampliar los ingresos? ¿Creará la nube nuevas eficiencias?
- Evalúe los aspectos económicos de una nube privada vs una pública. Las diferencias económicas pueden ser significativas, en base a requerimientos individuales, mientras que se deben administrar activamente los riesgos, como la seguridad.
- Mida los riesgos vs los beneficios a medida que evalúa las afirmaciones y capacidades de los proveedores de nube.
- Entienda cuándo el proveedor de nube (interno o externo) forzará cambios en el proceso organizacional y evalúe las implicancias y el plan de administración de cambios. ¿Hay algún factor de rediseño organizacional que considerar? ¿Soporta su actual modelo operativo el plan de migración a la nube? Si no es así, ¿ha diseñado apropiadamente su modelo operativo objetivo?
- Enfóquese en descifrar y validar las afirmaciones de ahorro de costos del disco duro virtual. Pruebe estas afirmaciones contra el costo total de los cálculos de propiedad que incluyen las implicancias de cumplimiento, impuestos y administración de cambios. ¿Son estas únicas por organización? (A menudo son inexactas cuando las suministra un proveedor).

- Pruebe las necesidades de personalización organizacionales. Mientras más personalización se necesite, menor es la probabilidad de éxito de la nube. ¿Es crítica la personalización deseada?

- Defina los temas de integración del negocio, con énfasis específico en los datos que ahora pueden estar dispersos en toda la organización. Entienda cómo la arquitectura de los datos debe evolucionar para abordar la nube y la operatividad entre nubes y entre organizaciones.

- Evalúe el personal interno, los roles actuales y cambios necesarios y cuán bien las habilidades actuales se vinculan con el modelo de nube que se está diseñando o implementando.

- Considere si un proyecto de nube no ingresa en el proceso típico de presupuesto y aprobación de capital, ¿Existirá fuera de los modelos de gobierno corporativo? ¿Qué mecanismos existen para asegurar que se mantenga el gobierno corporativo?

- ¿Cómo influirá la continuidad del negocio y la recuperación de desastres en su estrategia de migración a la nube?

- Entienda el proceso de contratación. A medida que las ofertas se vuelven más estandarizadas, también lo hace el contrato. Asegúrese de que su organización pueda acomodarse a los requerimientos del proveedor y de entender qué es negociable. Entienda la extensión óptima del contrato de modo que su proyecto proporcione la flexibilidad necesaria para avanzar a medida que evoluciona el mercado.

- Recuerde considerar los Acuerdos de Nivel del Servicio y cómo se administrarán. ¿Existen los mecanismos adecuados en la estrategia de administración de su proveedor actual para administrar eficazmente los proyectos de nube?

- Evalúe la estrategia de riesgo administrativo de su proveedor bajo el lente de la nube. Los proveedores también están pasando por su propia transformación a modelos de entrega de nube, generando un impacto financiero y operacional significativo. Asegúrese de que su estrategia de administración mida apropiadamente la capacidad financiera del proveedor para reestructurar su modelo de negocios.

- Determine las necesidades de información de aseguramiento para su proveedor de nube. Los requerimientos que funcionaban para la externalización, pueden no suministrar la garantía que se necesita en un entorno de nube. Evalúe el cambio de probar un proceso completo vs una transacción y si es suficiente.

- No olvide las implicancias de auditoría interna, seguridad global y regulatorias de los datos (privacidad, almacenamiento, co-ubicación, nexos tributarios, etc. ¿Cómo audita usted el mundo compartido de la nube? ¿Cómo determina que se cumplen todos los requerimientos regulatorios? ¿Le dará su clave de encriptación de datos a su proveedor? ¿Se le exige a su proveedor revelar las violaciones de datos?

PROFESIONALES DE TI:

- Trabaje estrechamente con los líderes de unidad de negocios para desarrollar una estrategia integral de nube y un plan de acción. Cree la visión empresarial y un esquema para la nube. Identifique las oportunidades de prueba de concepto a aprovechar.

- ¿Son sus plataformas tecnológicas un acelerador o un inhibidor de su estrategia corporativa?

- Eduque a los líderes de las unidades de negocios sobre las capacidades realistas y el potencial de la nube desde una perspectiva de la TI.

- Acuda a especialistas competentes para estudiar el mercado de la nube, sus capacidades, ofertas y proveedores.

- Evalúe la interoperabilidad de las soluciones de nube en comparación con las aplicaciones, plataformas e infraestructura actuales. Evalúe su preparación para la migración a la nube. Asegúrese de que la evaluación sea objetiva.

- Redefina el rol del Director de Informática a medida que evoluciona del proveedor de TI al Director de Integración, quien tiene la oportunidad de generar modelos de negocios e innovación.

- Desarrolle planes para diversos escenarios de adopción y despliegue de la nube en cada una de sus capas y en todas las distintas áreas operativas de la TI y el negocio.

- Interprete los servicios y las capacidades de nube en el contexto de tener que contratarlos con terceros (por ejemplo, aumentar o disminuir la capacidad puede ser técnicamente más fácil de lo que permite el contrato con el proveedor).

- Diseñe, desarrolle y despliegue programas de gobierno operativo y administración de riesgos desde la perspectiva de la TI y los servicios de disco duro virtual.

PROFESIONALES DE NEGOCIOS

- Trabaje estrechamente con los líderes de TI para desarrollar una estrategia integral de nube y un plan de acción para asegurar que se administren los puntos de integración críticos y para garantizar que se aprovechen todas las oportunidades de eficiencia y eficacia.

- Enfóquese en el valor comercial y el potencial de la nube por sobre sus capacidades técnicas o méritos. Al mismo tiempo, trabaje con la organización de TI para evitar grupos aislados de capacidades que crearán conjuntos de datos dispares a administrar.

- Entienda los riesgos del despliegue de servicios de nube sin el aporte y apoyo del grupo de TI y en el contexto de la arquitectura de TI predominante (incluyendo los datos y otra arquitectura técnica).

- Evalúe las implicancias de desplegar “aplicaciones” más estandarizadas y menos personalizables ahora que su proceso de negocio está habilitado por un servicio.

- Desarrolle escenarios diversos para la adopción y el despliegue de la nube en las diferentes áreas operativas del negocio.

- Entienda si la nube es un mecanismo para reemplazar y/o modernizar las aplicaciones back-office.

PROFESIONALES DE RIESGO, AUDITORES INTERNOS Y COMITÉS DE IMPUESTO Y AUDITORÍA

- Asegúrese de que hayan profesionales con las destrezas adecuadas para evaluar y monitorear los aspectos de la administración de riesgo y controles de la nube.

- Incluya la consideración de riesgo y controles en el proceso de selección de la nube.

- Entienda que pueden no existir los controles de TI tradicionales en un proveedor de servicios de nube. Puede que ahora el financiamiento, el desarrollo y el ciclo de vida de la implementación requieran un nuevo modelo de gobierno.
- Entienda que los usuarios tienen acceso a servicios de nube pública y que se deben desarrollar políticas para proteger a su organización. Es poco realista pensar que sus empleados no acceden a estas herramientas públicas.
- Involucre a los grupos de riesgo, auditoría y del comité de auditoría en los procesos de planificación y selección de servicios de nube. Exija informes periódicos sobre el monitoreo de la administración de riesgo y controles en servicios de nube desplegados.
- Evalúe cómo se asegurará la información y se mantendrá la confidencialidad.
- Determine cómo la adopción del disco duro virtual afectará los requerimientos regulatorios y de cumplimiento.
- Establezca un programa formalizado de aseguramiento, ya sea mediante Auditoría Interna o informes de aseguramiento independiente (informes SOC).
- Entienda las implicancias tributarias globales, regionales y locales del entorno de nube.

ANEXO 2: CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE (CSA CAIA v.3.0.1)

Adaptado al Modelo de Gestión de Riesgos de Infraestructura como Servicios (IaaS) de Cloud Computing para Empresas del Sector Publico Ecuatoriano, a fin de determinar qué medidas de seguridad, procedimientos y procesos de seguridad han implementado el proveedor de nube candidato:

GRUPO DE CONTROL	DETALLE	PREGUNTAS	RESPUESTAS			MAPEO	
			SI	No	NO APLICABLE	COBIT 5.0	ISO/IEC 27001:2005
Seguridad de Aplicaciones e Interfaces. *Requerimientos de acceso de clientes*	Antes de conceder a los clientes el acceso a los datos, activos y sistemas de información, todos los requisitos identificados de seguridad, contractuales y reglamentarios sobre el acceso de los clientes deberán ser considerados y corregidos.	¿Todos los requerimientos de seguridad, contractual y regulatorios son direccionados y remediados previo a la concesión de acceso a los datos, bienes y sistemas de información por parte del cliente?				APO09.01 APO09.02 APO09.03 APO13.01 BAI02 DSS05	A.6.2.1 A.6.2.2 A.11.1.1
		¿Todos los requerimientos y niveles de confianza son definidos y documentados para el acceso de los usuarios?					
Cumplimiento y aseguramiento de las Auditorías. *Auditorías Independientes*	Las revisiones independientes y las evaluaciones se llevarán a cabo al menos anualmente, o en intervalos planificados, para asegurarse de que la organización resuelve cualquier no conformidad de las políticas establecidas, los procedimientos y el cumplimiento de las obligaciones contractuales, estatutarias o reguladoras.	¿Permite a los inquilinos ver su SCO2/ISO 27001 o informes similares de auditoria o certificación de terceros?				APO12.04 APO12.05 DSS05.07 MEA02.06 MEA02.07 MEA02.08 MEA03.01	Clause 4.2.3e Clause 5.1 g Clause 5.2.1 d) Clause 6 A.6.1.8
		¿Realiza pruebas de penetración de la red de servicios de infraestructura en la nube con regularidad según lo prescrito por las mejores prácticas y la orientación de la industria?					
		¿Realiza pruebas de penetración de aplicaciones de servicios de infraestructura					

		en la nube con regularidad según lo prescrito por las mejores prácticas y la orientación de la industria?					
		¿Realiza auditorías internas regularmente según lo prescrito por las mejores prácticas y la orientación de la industria?					
		¿Realiza auditorías externas con regularidad según lo prescrito por las mejores prácticas y la orientación de la industria?					
		¿Los resultados de las pruebas de penetración están disponibles de acuerdo al requerimiento de los inquilinos?					
		¿Los resultados de auditorías internas y externas están disponibles de acuerdo al requerimiento de los inquilinos?					
		¿Disponen de un programa de auditoria que permite evaluaciones de auditoria multidisciplinarias?					
Cumplimiento y aseguramiento de las Auditorías. *Mapa de regulación de los sistemas de información*	Se deberá mantener un inventario de las obligaciones externas legales, estatutarias y reglamentarias de la organización asociado (y mapeado) con cualquier alcance y presencia geográfica, y que considere datos relevantes o información propiedad de la organización y administrada por la infraestructura de red (física o virtual) y los componentes de los sistemas, actualizado periódicamente según las	¿Tiene la capacidad de segmentar lógicamente o cifrar los datos de los clientes talque los datos puede ser producido por un solo inquilino, sin acceder inadvertidamente hacia los datos de otro inquilino?				APO12.01 APO12.02 APO12.03 MEA03.01	Clause 4.2.1 b) 2) Clause 4.2.1 c) 1) Clause 4.2.1 g) Clause 4.2.3 d) 6) Clause 4.3.3 Clause 5.2.1 a – f Clause 7.3 c) 4)
		¿Tiene la capacidad de recuperar los datos de un cliente específico en el caso de una pérdida o fallo de datos?					

	necesidades del negocio (por ejemplo, un cambio en el alcance y/o un cambio en las obligaciones).	¿Tiene la capacidad de restringir el almacenamiento de datos de los clientes a países específicos o ubicaciones geográficas?					A.7.2.1 A.15.1.1 A.15.1.3
		¿Se dispone de un programa con la capacidad de monitorear los cambios en los requisitos reguladores de las jurisdicciones pertinentes, ajuste su programa de seguridad para los cambios en los requisitos legales, y garantizar el cumplimiento de los requisitos reglamentarios pertinentes?					A.15.1.4 A.15.1.6
Gestión de la Continuidad del Negocio y Resiliencia Operacional. *Planificación de la Continuidad de Negocio*	Debe establecerse un marco unificado y consistente para la planificación de la continuidad de negocio y debe desarrollarse un plan, documentado y adaptado, para asegurar que todos los planes de continuidad del negocio son consistentes en el tratamiento de las prioridades, las pruebas, el mantenimiento y los requisitos de seguridad de la información. Los requisitos para los planes de continuidad del negocio deben incluir los siguientes: • Un propósito y alcance definidos y en línea con las dependencias pertinentes • Accesible y comprensible para los que van a utilizarlos • Identificación de una(s) persona(s) nombrada(s) que es(son) responsable(s) de su revisión, actualización y aprobación • Las líneas de comunicación específicas, los roles y las responsabilidades deberán estar definidos	¿Provee a los inquilinos opciones de alojamiento geográficamente resilentes?				DSS04.01 DSS04.02	Clause 5.1 A.6.1.2
		¿Provee a los inquilinos capacidad de migración por error de servicios de infraestructura a otros proveedores?				DSS04.03 DSS04.05	A.14.1.3 A.14.1.4

	• Los procedimientos de recuperación, los manuales de trabajo y la información de referencia están detallados. • Hay un método para la invocación del plan						
Gestión de la Continuidad del Negocio y Resiliencia Operacional. *Pruebas de Continuidad de Negocio*	Los planes de respuesta ante incidentes de seguridad y de continuidad de negocio estarán sometidos a pruebas en los intervalos planificados o cuando se produzcan cambios organizativos o ambientales significativos. Los planes de respuesta ante incidentes deberán implicar a los clientes (arrendatarios) afectados y a otras relaciones comerciales que representen dependencias críticas de procesos de negocio dentro de la cadena de suministro.	¿Los planes de continuidad del negocio son sujetos de prueba a intervalos planificados o en cambios organizativos o ambientales significativos para garantizar la eficacia continua?				DSS04.04	A.14.1.5
Gestión de la Continuidad del Negocio y Resiliencia Operacional. *Análisis de Impacto*	Deberá existir un procedimiento definido y documentado para determinar el impacto de cualquier interrupción en la organización, que deberá incorporar los siguientes aspectos: • Identificar los productos y servicios críticos • Identificar todas las dependencias, incluyendo procesos, aplicaciones, socios comerciales y proveedores de servicios externos • Comprender las amenazas a los productos y servicios críticos • Determinar los impactos resultantes de interrupciones planificadas o no planificadas y cómo éstos varían con el tiempo Establecer el período máximo tolerable de interrupción • Establecer prioridades para la recuperación	¿Provee a los inquilinos de visualización y reporte continuo del rendimiento operación de su Acuerdo de Nivel de Servicio (SLA)?				BAI06.01 BAI10.01 BAI10.02 BAI10.03 DSS04.01 DSS04.02	A.14.1.2 A 14.1.4
		¿Las métricas para seguridad de la información basada en estándares (CSA, GMAO, etc.) se encuentran a disposición de los inquilinos?					
		¿Provee al cliente reporte y visualización continua del rendimiento de su SLA?					

	• Establecer los objetivos de tiempo de recuperación para la reanudación de los productos y servicios críticos dentro de su período máximo tolerable de interrupción • Estimar los recursos necesarios para la reanudación						
Seguridad del Centro de Datos. *Equipamiento fuera de las instalaciones*	Se deberá establecer políticas y procedimientos apoyando los procesos de negocio implementados para el uso y eliminación segura del mantenimiento de equipos y el uso fuera de las instalaciones de la organización.	¿Proporciona a los inquilinos evidencia documentada respecto a las políticas y procedimientos que gobiernan la gestión de activos y reutilización de equipos?				APO09.03 APO10.04 APO10.05 APO13.01 DSS01.02	A.9.2.5 A.9.2.6
Gobierno y Gestión del Riesgo. *Programa de Gestión*	Un programa de gestión en seguridad de la información debe estar desarrollado, documentado, aprobado, e implementado, incluyendo medidas administrativas, técnicas y físicas para proteger activos y datos de la pérdida, el acceso no autorizado, el uso indebido, la divulgación, la alteración y la destrucción. El programa de seguridad debe incluir, pero no debe estar limitado, por las siguientes áreas, desde el momento en que éstas están relacionadas con las características del negocio: • Gestión de riesgos • Política de seguridad • Organización de la seguridad de la información • Gestión de activos • Seguridad de recursos humanos • Seguridad física y del entorno • Gestión de comunicaciones y operaciones • Control de acceso	¿Provee a los inquilinos documentación que describe su Programa de Gestión de Seguridad de la Información (ISMP)?				APO13.01 APO13.02 APO13.03	Clause 4.2 Clause 5 A.6.1.1 A.6.1.2 A.6.1.3 A.6.1.4 A.6.1.5 A.6.1.6 A.6.1.7 A.6.1.8

	• Adquisición de sistemas de información, desarrollo y mantenimiento.						
		¿Revisa el Programa de Gestión de Seguridad de la Información (ISMP) por lo menos una vez al año?					
Gobierno y Gestión del Riesgo. *Impacto de la Política en las Evaluaciones del Riesgo*	Los resultados de la evaluación de riesgos deberán incluir actualizaciones de las políticas de seguridad, de los procedimientos, de las normas y los controles, para asegurar que estos documentos permanecen relevantes y efectivos.	¿Los resultados de la evaluación de riesgos incluyen actualizaciones a las políticas, procedimientos, normas y controles de seguridad para garantizar que sigan siendo relevantes y eficaces?				APO12 APO13.01 APO13.03	Clause 4.2.3 Clause 4.2.4 Clause 4.3.1 Clause 5 Clause 7 A.5.1.2 A.10.1.2 A.10.2.3 A.14.1.2 A.15.2.1 A.15.2.2
Gobierno y Gestión del Riesgo. *Análisis de Riesgo*	Un análisis de riesgos formalizado, alineado con los objetivos de la organización, deberá ser realizado al menos una vez al año o a intervalos planificados para determinar la probabilidad e impacto de todos los riesgos identificados, usando métodos cuantitativos o cualitativos. La probabilidad y el impacto asociado con el riesgo intrínseco y residual deberá estar determinado independientemente, considerando todas las categorías de riesgo (por ejemplo, con el resultado de las auditorías, el análisis de vulnerabilidades y amenazas y el cumplimiento normativo).	¿Las evaluaciones de riesgo están formalizados y alineados con el marco de trabajo de toda la organización, y se lo realiza anualmente o en intervalos planificados, para determinar la probabilidad y el impacto de todos los riesgos identificados, utilizando métodos cualitativos y cuantitativos?				APO12	Clause 4.2.1 c) – g) Clause 4.2.3 d) Clause 5.1 f) Clause 7.2 & 7.3 A.6.2.1 A.12.5.2 A.12.6.1 A.14.1.2 A.15.1.1 A.15.2.1 A.15.2.2
		¿La probabilidad y el impacto asociado con el riesgo inherente y residual se determinan de manera independiente, teniendo en cuenta todas las categorías de riesgo (por ejemplo,					

		resultados de las auditorías, análisis de amenazas y vulnerabilidad, y el cumplimiento normativo)?					
Governance and Risk Management *Program*	Las organizaciones desarrollarán y mantendrán un sistema de gestión de riesgos para mitigar el riesgo a un nivel aceptable.	¿Se dispone de un programa documentado de toda la organización establecido para manejar el riesgo?				EDM03.02 APO01.03 APO12	Clause 4.2.1 c) – g) Clause 4.2.2 b) Clause 5.1 f) Clause 7.2 & 7.3 A.6.2.1 A.12.6.1 A.14.1.2 A.15.2.1 A.15.2.2
		¿Se documenta y se tiene acceso al programa de gestión de riesgos en toda la organización?					
Human Resources *Asset Returns*	A la finalización del contrato de trabajo y/o la finalización de las relaciones comerciales externas, los activos propiedad de la organización deben ser devueltos dentro del periodo establecido.	¿Están los sistemas establecidos para monitorear violaciones a la privacidad y notificar con rapidez a los inquilinos si un evento de privacidad puede haber afectado sus datos?				APO01.08 APO07.06 APO13.01 BAI09.03	A.7.1.1 A.7.1.2 A.8.3.2
		¿Están las políticas de privacidad alineados con los estándares de la industria?					
Recursos Humanos. *Contratos laborales*	Los contratos laborales deberán incorporar las cláusulas y/o los términos de cumplimiento para establecer el gobierno de la información y las políticas de seguridad y deberán ser firmados en las nuevas contrataciones o por el nuevo personal (por ejemplo, empleados a tiempo total o parcial o trabajadores eventuales), y siempre con anterioridad a proporcionar el acceso al usuario a los servicios de la organización, recursos y activos.	¿Está el personal entrenado respecto a sus funciones específicas y a los controles de seguridad de la información que deben cumplir?				APO01.03 APO13.01 APO07.06 APO09.03 APO10.01	A.6.1.5 A.8.1.3
		¿Se documenta o registra una vez finalizada el entrenamiento del empleado?					
		¿Todo el personal firma un Acuerdo de Confidencialidad (NDA) como condición de					

		empleo para proteger la información del cliente/inquilino?					
		¿Haber culminado oportunamente los programas de formación es considerado un requisito previo para la adquisición y mantenimiento de los sistemas de información sensibles, por parte del proveedor?					
		¿El personal ha sido capacitado y dotada en programas de concienciación al menos una vez al año?					
Human Resources *Employment Termination*	Roles and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and communicated.	¿Las políticas, procedimientos y directrices para la gestión del cambio o terminación de relaciones laborales se encuentran documentadas?				APO01.02 APO07.05 APO07.06	A.8.3.1
		¿Cuenta de procedimientos y directrices apropiadas para la revocación oportuna de acceso y retorno de los activos?					
Recursos Humanos. *Gestión de dispositivos móviles*	Se establecerán las políticas y los procedimientos y se implementarán las medidas técnicas de apoyo para gestionar el riesgo de negocio asociado a que esté permitido que los dispositivos móviles accedan a recursos corporativos, pudiendo requerir de la implementación o controles compensatorios de seguridad más altos para su uso aceptable (por ejemplo, formación por mandato de seguridad, autenticación fuerte, derechos y controles de acceso y monitorización de dispositivos).	¿Se encuentran establecidas las políticas y procedimientos y las medidas aplicadas para limitar estrictamente el acceso a sus datos confidenciales y los datos de los inquilinos desde dispositivos portátiles y móviles (por ejemplo, ordenadores portátiles, teléfonos celulares y asistentes digitales personales (PDA)), que generalmente son de mayor riesgo que los dispositivos no portátiles (por				APO01.08 APO13.01 APO13.02 DSS05.01 DSS05.02 DSS05.03 DSS05.07 DSS06.03 DSS06.06	A.7.2.1 A.10.7.1 A.10.7.2 A.10.8.3 A.11.7.1 A.11.7.2 A.15.1.4

		ejemplo, las computadoras de escritorio en las instalaciones de la organización profesional)?					
Recursos Humanos. *Roles / Responsabilidades*	Los roles y responsabilidades de contratistas, empleados y terceras partes deberán estar documentadas en lo que respecta a los activos de información y seguridad.	¿Se provee a los inquilinos o arrendatarios de un documento de definición de roles y responsabilidades en la cual se establece sus responsabilidades administrativas?				APO01.02 APO01.03 APO01.08 APO07.06 APO09.03 APO10.04 APO13.01 APO13.03	Clause 5.1 c) A.6.1.2 A.6.1.3 A.8.1.1
Recursos Humanos. *Formación / Concienciación*	Un programa de concienciación debe establecerse para todos los proveedores, usuarios de terceras-partes y empleados de la organización y exigido cuando sea conveniente. Todas las personas con acceso a datos de la organización recibirán una formación de forma regular en procedimientos de la organización, procesos y políticas relacionada con su función profesional respecto a la organización.	¿Se ofrecen un programa de entrenamiento formal, basado en roles, conciencia de seguridad para el acceso relacionados con la nube y los problemas de gestión de datos (por ejemplo, multiempresa, nacionalidad, nube modelo de prestación de segregación de funciones implicaciones y conflictos de intereses) para todo el personal con acceso a datos de los inquilinos?				APO01.03 APO01.08 APO07.03 APO07.06 APO13.01 APO13.03	Clause 5.2.2 A.8.2.2
		¿Los administradores y sus auxiliares son instruidos adecuadamente sobre sus responsabilidades legales en materia de seguridad e integridad de los datos?					
Recursos Humanos. *Responsabilidad de los Usuarios*	Se deberá hacer consciente a todo el personal de sus roles y responsabilidades para:	¿Son los usuarios conscientes de sus responsabilidades para mantener la conciencia y el cumplimiento de políticas y				APO01.02 APO01.03 APO01.08	Clause 5.2.2

	Mantener el cumplimiento y concienciación respecto a las políticas y procedimientos establecidos así como con la legislación aplicable y obligaciones de cumplimiento regulatorio. • Mantener un entorno de trabajo seguro.	procedimiento de seguridad, así como, las normas y los requisitos reglamentarios aplicables?				APO07.03 APO07.06 APO13.01 APO13.03	A.8.2.2 A.11.3.1 A.11.3.2
		¿Son los usuarios conscientes de sus responsabilidades para mantener un ambiente de trabajo seguro y protegido?					
		¿Son los usuarios conscientes de sus responsabilidades por dejar el equipo desatendido de forma segura?					
Recursos Humanos. *Lugares de trabajo*	Las políticas y procedimientos establecerán requerimientos para que en los lugares de trabajo sin personal presente no existan (por ejemplo, sobre la mesa) documentos de contenido sensible totalmente accesibles y las sesiones de usuario iniciadas en el equipo informático hayan sido bloqueadas tras un período determinado de inactividad.	¿Las políticas y procedimientos de gestión de datos están dirigidas a conflictos de interés entre inquilino y los nivel de servicio?				APO01.02 APO01.03 APO01.08 APO07.03 APO07.06 APO13.01 APO13.03 DSS05.03 DSS06.06	Clause 5.2.2 A.8.2.2 A.9.1.5 A.11.3.1 A.11.3.2 A.11.3.3
		¿Las políticas y procedimientos de gestión de datos incluyen una auditoría anti sabotaje o funciones de integridad software para el acceso no autorizado a los datos inquilino?					
		¿La infraestructura de administración de máquinas virtuales incluye una auditoría anti sabotaje o funciones de integridad del software para detectar cambios en la construcción / configuración de máquinas virtuales?					
Gestión de Identidades y Accesos. *Acceso por Terceros*	La identificación, evaluación y priorización de los riesgos planteados por los procesos de negocio que requieren acceso de terceros a los datos y sistemas de información de la organización deberán ir seguidos de la aplicación coordinada de recursos para minimizar, monitorizar y medir la	¿Proporciona la capacidad de recuperación de desastres múlti-fracaso?				APO01.03 APO01.08 APO07.06 APO10.04 APO13.02	A.6.2.1 A.8.3.3 A.11.1.1 A.11.2.1 A.11.2.4
		¿Monitorea la continuidad del servicio con otros proveedores en caso de fallo de proveedor?					

	probabilidad y el impacto de accesos no autorizados o inapropiados. Los controles compensatorios derivados del análisis de riesgos se implantarán antes de la provisión de acceso.	¿Tiene más de un proveedor por cada servicio que depende?				DSS05.04 DSS05.07 DSS06.03 DSS06.06	
		¿Provee acceso continuo y redundante, incluyendo los servicios de los que depende?					
		¿Proporciona el inquilino la posibilidad de declarar un desastre?					
		¿Provee la capacidad de recuperación por error desencadenada por el arrendatario o inquilino?					
		¿Comparte la continuidad de negocio y planes de redundancia con los inquilinos o arrendatarios?					
Seguridad de la Infraestructura y Virtualización. *Seguridad Inalámbrica*	Se establecerán políticas y procedimientos, así como apoyo a los procesos de negocio y las medidas técnicas implementadas, para proteger los entornos de red inalámbrica, incluyendo las siguientes: • Firewalls perimetrales implementados y configurados para restringir el tráfico no autorizado	¿Las políticas y procedimientos están establecidos, al igual que los mecanismos para proteger el entorno de red perimetral inalámbrica se encuentran configurados e implementados para restringir el tráfico inalámbrico no autorizado?				APO01.08 APO13.01 APO13.02 DSS02.02 DSS05.02 DSS05.03	A.7.1.1 A.7.1.2 A.7.1.3 A.9.2.1 A.9.2.4 A.10.6.1
	• Configuraciones de seguridad habilitadas con cifrado robusto para la autenticación y transmisión reemplazando la configuración por defecto del fabricante (por ejemplo, claves de cifrado, contraseñas y SNMP "community strings") • Acceso de usuario a dispositivos de red inalámbricos restringido a personal autorizado	¿Políticas y procedimientos están establecidos, al igual que los mecanismos para asegurar la configuración de seguridad inalámbricas se encuentran implementados y activadas con una fuerte encriptación para la autenticación y transmisión, en sustitución de la configuración predeterminada del proveedor? (por ejemplo, claves de cifrado, contraseñas, cadenas de comunidad SNMP)				DSS05.04 DSS05.05 DSS05.07 DSS06.03 DSS06.06	A.10.6.2 A.10.8.1 A.10.8.3 A.10.8.5 A.10.10.2 A.11.2.1 A.11.4.3 A.11.4.5 A.11.4.6

	• Capacidad de detectar la presencia de dispositivos de red inalámbricos no autorizados (rogue) para una desconexión oportuna de la red	¿Las políticas y procedimientos están establecidos, al igual que los mecanismos para proteger los entornos de red inalámbrica y detectar la presencia de dispositivos de red no autorizadas por una desconexión puntual de la red se encuentran implementados?					A.11.4.7 A.12.3.1 A.12.3.2
Gestión de incidentes de seguridad, Localización de evidencias electrónicas, Investigaciones forenses en la nube *Puntos de contacto con las autoridades*	Se deberán mantener disponibles y actualizados los puntos de contacto de las fuerzas de seguridad locales y nacionales, autoridades legislativas aplicables y otras autoridades con jurisdicción legal (sobre todo en caso de cambios en el alcance o en las obligaciones de cumplimiento), de modo que se asegure el establecimiento directo de los enlaces correspondientes y la disposición para una investigación forense que requiera una participación rápida de las fuerzas de seguridad.	¿Se mantiene enlaces y puntos de contacto con las autoridades locales de acuerdo con los contratos y reglamentos apropiados?				APO01.01 APO01.02 APO01.03 APO01.08 MEA03.01 MEA03.02 MEA03.03	A.6.1.6 A.6.1.7
Gestión de incidentes de seguridad, Localización de evidencias electrónicas, Investigaciones forenses en la nube *Gestión de incidentes*	Se deberán establecer procedimientos y políticas, así como medidas técnicas y procesos de negocio de apoyo, que permitan la evaluación y clasificación de eventos de seguridad y que garanticen una gestión completa y en tiempo de los incidentes así como sea establecido en las políticas y procedimientos de gestión de servicios TI.	¿Se dispone de un plan de respuesta a incidentes de seguridad documentado?				APO01.03 APO13.01 APO13.02 DSS01.03 DSS02.01 DSS02.02 DSS02.04 DSS02.05 DSS02.06	Clause 4.3.3 A.13.1.1 A.13.2.1
		¿Integra requisitos personalizadas del arrendatario o huésped en sus planes de respuesta a incidentes de seguridad?					
		¿Publican el documento de funciones y responsabilidades en la que se especifica las responsabilidades de los arrendatarios o huéspedes durante los incidentes de seguridad?					

		¿Se ha Validado el plan de respuesta a incidentes de seguridad en el último año?					
Gestión de incidentes de seguridad, Localización de evidencias electrónicas, investigaciones forenses en la nube *Comunicación de incidentes*	Se deberá informar a los trabajadores y a las empresas externas relacionadas acerca de sus responsabilidades y, si fuera necesario, deberán dar su consentimiento o aceptar contractualmente a informar prontamente de todos los eventos de seguridad. Los eventos de seguridad deberán ser comunicados a través de canales de comunicación predefinidos oportunamente cumpliendo con las obligaciones legales, reglamentarias o de cumplimiento regulatorio aplicables.	¿El sistema de gestión de eventos e incidentes de seguridad (SIEM) combina las fuentes de datos (registros de aplicaciones, los registros del firewall, IDS registros, registros de acceso físico, etc.) para una análisis granular y de alerta?				APO01.03 APO07.06 APO07.03 APO13.01 APO13.02 DSS02.01	Clause 4.3.3 Clause 5.2.2 A.6.1.3 A.8.2.1 A.8.2.2 A.13.1.1 A.13.1.2 A.13.2.1
		¿El marco de trabajo de monitoreo y registro permite el aislamiento de un incidente por arrendatario o huésped especifico?					
Gestión de incidentes de seguridad, Localización de evidencias electrónicas, investigaciones forenses en la nube *Preparaciones legales para la respuesta ante incidentes*	En el caso de que una investigación posterior que afecte a una persona u organización después de un incidente de seguridad requiera acciones legales se exige el seguimiento de los debidos procedimientos forenses, incluyendo la cadena de custodia, para la preservación y presentación de las pruebas que apoyen dichas acciones legales ante la jurisdicción pertinente. Tras la notificación, los clientes (arrendatarios) y/o las relaciones con otras empresas externas que hayan sido afectadas por una violación de seguridad deberán tener la oportunidad de participar como sea legalmente posible en la investigación forense.	¿El plan de respuesta a incidentes cumple con estándares legalmente admitida por la industria para la gestión de los procesos y controles de la cadena de custodia?				APO01.03 APO13.01 APO13.02 DSS01.03 DSS02.01 DSS02.02 DSS02.04 DSS02.05 DSS02.06	Clause 4.3.3 Clause 5.2.2 A.8.2.2 A.8.2.3 A.13.2.3 A.15.1.3
		¿La capacidad de respuesta a incidentes incluye el uso de técnicas de recolección y análisis de datos forenses legalmente admitidas?					
		¿Existe la capacidad de soportar conservación de material (congelación de los datos de un punto específico en el tiempo) para un inquilino específico sin congelar los datos de otro inquilino?					
		¿Da fe y cumple con la separación de datos en producción de los inquilinos en respuesta a citaciones legales?					

Gestión de incidentes de seguridad, Localización de evidencias electrónicas, investigaciones forenses en la nube *Métricas de la respuesta ante incidentes*	Se deberán implantar los mecanismos que permitan monitorizar y cuantificar los tipos, cantidades y costes de los incidentes de seguridad de la información.	¿Se monitorea y cuantifica los tipos, volúmenes y los impactos sobre todos los incidentes de seguridad de la información?				DSS04.07	A.13.2.2
		¿Se comparte información estadística de los incidentes de seguridad con los inquilinos que lo soliciten?					
Gestión de la cadena de suministro, Transparencia y Responsabilidad *Servicios de red / infraestructura*	Los componentes de la infraestructura de sistemas y redes, así como el diseño y configuración de las aplicaciones (físicas y virtuales) y de los interfaces sistema-sistema (API) que sean críticos para el negocio o que impacten al cliente (arrendatario) deberán ser diseñados, desarrollados y desplegados de acuerdo con unas expectativas de nivel de servicio y capacidad acordadas previamente, así como de acuerdo a las políticas y procedimientos de gestión de servicio y gobernanza TI.	¿Se dispone de la capacidad de recoger y usar la información relevante de los componentes de su Proveedor de Nube?				APO01.03 APO03.01 APO03.02 APO09.03 BAI02.01 BAI02.04 BAI07.05	A.6.2.3 A.10.6.2
		¿Se provee a los inquilinos la capacidad de planificación y uso de reportes?					
Supply Chain Management, Transparency and Accountability *Provider Internal Assessments*	The provider shall perform annual internal assessments of conformance and effectiveness of its policies, procedures, and supporting measures and metrics.	¿Se realiza evaluaciones internas anuales de conformidad y eficacia de sus políticas, procedimientos y de la métricas y medidas de apoyo?				MEA01 MEA02	
Gestión de la cadena de suministro,	Los Acuerdos de la cadena de suministro (por ejemplo, SLA) entre proveedores y clientes (arrendatarios) contendrán al	¿Se selecciona y monitorea la subcontratación de proveedores de				APO09.03 APO09.05	A.6.2.3 A10.2.1

Transparencia y Responsabilidad *Acuerdos relativos a la cadena de suministro*	menos las siguientes mutuamente acordadas disposiciones y/o los términos: • Alcance de la relación comercial y de servicios que se ofrece (por ejemplo , adquisición de datos del cliente (arrendatario), el intercambio y el uso, conjuntos de características y funcionalidad , el personal y la infraestructura de red y componentes de los sistemas de prestación de servicios y apoyo, roles y responsabilidades de proveedor y cliente (arrendatario) y cualquier relación comercial subcontratada o externalizada, la ubicación geográfica física de los servicios de hospedaje , y cualquier aspecto de cumplimiento regulatorio conocidos) • Los requisitos de seguridad de la información, los puntos de contacto principales durante la duración de la relación comercial del proveedor y el cliente (arrendatario), y las referencias a la información detallada de apoyo y procesos de negocio relevantes y medidas técnicas implementadas para permitir el gobierno efectivo, la gestión de riesgos y cumplimiento de las obligaciones de seguridad, legales, estatutaria y normativas por todas las partes afectadas. • Notificación y/o pre- autorización los cambios controlados por el proveedor con impacto en el cliente (arrendatario)	conformidad a las leyes del país en que se procesan, almacenan o se trasmite los datos?					A.10.8.2 A.11.4.6 A.11.6.1 A.12.3.1 A.12.5.4
		¿Se selecciona y monitorea la subcontratación de proveedores de conformidad al cumplimiento de las leyes del país donde se originan los datos?					
		¿El asesor legal revisa todos los acuerdos de terceros?					
		¿Los acuerdos de terceros incluyen disposiciones para la seguridad y protección de la información y de los activos?					
		¿Se proporciona al cliente una lista y copias de todos los acuerdos procesados y lo mantiene actualizado?					

	• La notificación a tiempo de un incidente de seguridad (o brecha de seguridad confirmada) a todos los clientes (arrendatarios) y otras partes afectadas (es decir, hacia arriba y debajo de la cadena de suministro afectada) • Evaluación y verificación independiente del cumplimiento de las disposiciones del acuerdo y / o términos (por ejemplo, la certificación aceptable para la industria, el informe de auditoría de certificación, o formas equivalentes de aseguramiento) sin representar un riesgo de negocio inaceptable de la exposición para la organización que está siendo evaluada • Finalización de la relación comercial y el tratamiento de los datos del cliente (arrendatario) afectados • El cliente (arrendatario) de una aplicación servicio a servicio (API) y los requerimientos de interoperabilidad y portabilidad de los datos para el desarrollo de aplicaciones y el intercambio de información, el uso y la persistencia de la integridad.						

ANEXO 3: DIVISIÓN DE RESPONSABILIDADES

Considerando los incidentes de seguridad, es necesario que haya una definición y comprensión clara entre el cliente y el proveedor de los roles y responsabilidades de seguridad pertinentes, misma que varían mucho entre modelos de servicios SaaS y/o IaaS, este último delega más responsabilidad al cliente. En todo caso, para cada tipo de servicio, el cliente y el proveedor deben definir claramente su nivel responsabilidad, siendo potestad del cliente de nube verificar lo que se encuentra dentro de su responsabilidad.

ORGANIZACIÓN	CSP
SOFTWARE AS A SERVICE	
• Compliance with data protection law in respect of customer data collected and processed • Maintenance of identity management system • Management of identity management system • Management of authentication platform (including enforcing password policy)	• Physical support infrastructure (facilities, rack space, power, cooling, cabling, etc) • Physical infrastructure security and availability (servers, storage, network bandwidth, etc) • OS patch management and hardening procedures (check also any conflict between customer hardening procedure and provider security policy) • Security platform configuration (Firewall rules, IDS/IPS tuning, etc) • Systems monitoring • Security platform maintenance (Firewall, Host IDS/IPS, antivirus, packet filtering) • Log collection and security monitoring
PLATFORM AS A SERVICE	
• Maintenance of identity management system • Management of identity management system	• Physical support infrastructure (facilities, rack space, power, cooling, cabling, etc)

• Management of authentication platform (including enforcing password policy)	• Physical infrastructure security and availability (servers, storage, network bandwidth, etc) • OS patch management and hardening procedures (check also any conflict between customer hardening procedure and provider security policy) • Security platform configuration (firewall rules, IDS/IPS tuning, etc) • Systems monitoring • Security platform maintenance (firewall, Host IDS/IPS, antivirus, packet filtering) • Log collection and security monitoring
INFRASTRUCTURE AS A SERVICE	
• Maintenance of identity management system • Management of identity management system • Management of authentication platform (including enforcing password policy) • Management of guest OS patch and hardening procedures (check also any conflict between customer hardening procedure and provider security policy) • Configuration of guest security platform (firewall rules, IDS/IPS tuning, etc) • Guest systems monitoring • Security platform maintenance (firewall, Host IDS/IPS, antivirus, packet filtering) • Log collection and security monitoring	• Physical support infrastructure (facilities, rack space, power, cooling, cabling, etc) • Physical infrastructure security and availability (servers, storage, network bandwidth, etc) • Host Systems (hypervisor, virtual firewall, etc)

ANEXO 4: CLAUSULAS CONTRATOS DE NUBE

De acuerdo a la “Normativa para Contratos en la Nube” de la ENISA [15] se identifican las siguientes cláusulas contractuales que podrían ser empleadas y modificadas por los diferentes entidades de la Administración Publica Ecuatoriana. Donde:

- Contratista: Proveedor de Servicios de Nube
- Contratante: Entidad Gubernamental.

CLÁUSULAS

1. Confidencialidad y protección de datos.

Para los efectos de la presente cláusula, “Información Confidencial” constituye toda información, sea completa o parcial, sea verbal o escrita, independiente del medio en que conste o se transmita, que la CONTRATISTA recibe desde el CONTRATANTE en virtud del presente contrato o que la CONTRATISTA tome conocimiento por cualquier medio y ya sea que se refiera al CONTRATANTE, otros órganos públicos, sus autoridades, funcionarios, contratistas u otras personas.

La Información Confidencial del CONTRATANTE será mantenida en estricta reserva por la CONTRATISTA, quien deberá mantener la debida confidencialidad de los datos, bases de datos, documentos y a todos los archivos informáticos a que tenga acceso con motivo del presente contrato, quedándole expresamente prohibido divulgarlos, publicarlos, fotocopiarlos, copiarlos o distribuirlos a terceros extraños a este contrato o hacer cualquier uso indebido de ellos. Estas informaciones y datos sólo podrán ser revelados por instrucción del CONTRATANTE.

La CONTRATISTA guardará especial atención a la confidencialidad de los datos personales a que pueda tener acceso en virtud del presente contrato. En este sentido, la CONTRATISTA no podrá recolectar, almacenar, transferir, transmitir, comunicar, tratar, ceder o usar, de cualquier forma, los datos indicados anteriormente, salvo que dichas acciones sean indispensables para el cumplimiento de las obligaciones consignadas en el presente contrato y/o que medie una autorización escrita por parte del representante legal del

CONTRATANTE. En ningún caso se entenderá que la CONTRATISTA tiene algún derecho sobre tales datos personales.

La CONTRATISTA adoptará todas las medidas conducentes a resguardar la confidencialidad de la información por parte de su personal, incluyendo profesionales, consultores, contratistas o demás personas que deban tomar, hayan tomado o tengan conocimiento de la Información Confidencial del CONTRATANTE. Los consultores y personal dependiente de la CONTRATISTA, que de una u otra manera se hayan vinculado a la ejecución de los servicios contratados, en cualquiera de sus etapas, deberán guardar confidencialidad de la misma forma aplicable al CONTRATISTA. La responsabilidad de la CONTRATISTA en este ámbito, será solidaria respecto de la de sus administradores, representantes, personeros, empleados, consultores y todo aquel que se encuentre vinculado a la ejecución de los servicios contratados.

La divulgación, por cualquier medio, de la totalidad o parte de la información referida en los párrafos anteriores, por parte de la CONTRATISTA, durante la vigencia del contrato o una vez finalizado éste, podrá dar pie a que la CONTRATANTE entable en su contra las acciones judiciales que correspondan, sin perjuicio de la responsabilidad solidaria por los actos en infracción de esta obligación que hayan ejecutado sus empleados. Asimismo, lo anterior facultará al CONTRATANTE a informar a otros órganos públicos que tuvieren contratados servicios con la CONTRATISTA acerca de este incumplimiento.

Toda la Información Confidencial (incluyendo las copias tangibles y la almacenada por medios electrónicos y/o cualquier otro medio) proporcionada por el CONTRATANTE será devuelta a éste dentro de los 30 días corridos contados desde la recepción de un requerimiento escrito por el CONTRATANTE. Para dichos efectos, la CONTRATISTA entregará al CONTRATANTE todos los materiales que contengan o representen la Información Confidencial recibida. Hecho lo anterior, la CONTRATISTA no podrá mantener ninguna Información Confidencial del CONTRATANTE en su poder, debiendo eliminar de forma irreversible cualquier copia de dicha información que disponga en sus registros lógicos y físicos.

2. Seguridad de la información.

“La CONTRATISTA deberá adoptar todas las medidas técnicas y organizativas de seguridad que sean precisas para efectos de evitar que la información del CONTRATANTE sea accedida por terceros no autorizados.

Lo anterior se extiende, además, a las comunicaciones electrónicas de dicha información entre CONTRATISTA y el CONTRATANTE.

En tal caso, la CONTRATISTA deberá emplear las medidas de seguridad que sean necesarias para que estas comunicaciones no sean interceptadas.

Para lo anterior, seguirá los estándares de seguridad establecidos en las normas técnicas NTE INEN-ISO/IEC 27000

Asimismo, para efectos de claridad, se deja expresa constancia que la CONTRATISTA deberá adoptar las medidas de respaldo de la información que impidan que ésta se pierda como consecuencia de alguna contingencia que afecte sus sistemas informáticos.”

3. Responsabilidad Civil.

La responsabilidad civil de las partes derivadas de algún incumplimiento o cumplimiento parcial de las obligaciones establecidas en el presente contrato se regirá por las leyes de la República del Ecuador.

En ningún caso se entenderá que el CONTRATANTE acepta o admite alguna limitación convencional de responsabilidad por parte de la CONTRATISTA.

Finalmente, la CONTRATISTA será responsable de (1) cumplir con todas las leyes, reglamentaciones, ordenanzas y disposiciones gubernamentales vigentes que le fueren aplicables en la República del Ecuador y (2) de respetar los derechos de propiedad intelectual de terceras personas en la ejecución de las obligaciones establecidas en el presente instrumento.

La CONTRATISTA defenderá, indemnizará y mantendrán a salvo al CONTRATANTE de y en contra de cualquier reclamación, acción, demanda, y procedimiento legal (conjuntamente “Reclamo(s)”) y de toda responsabilidad, daño, pérdida, juicio, declaración autorizada, costos y gastos directos e indirectos (en adelante “Daños”) que surjan de o en relación con la violación de lo establecido en el presente contrato.

4. Propiedad Intelectual.

Toda la información, datos, documentos y bases de datos que la CONTRATISTA recibe desde el CONTRATANTE o que la CONTRATISTA toma conocimiento por cualquier medio en virtud del presente contrato serán de propiedad del CONTRATANTE y sólo podrá ser utilizado por la CONTRATISTA para efectos de la ejecución de las obligaciones emanadas en virtud del presente contrato. Cualquier otro uso estará prohibido salvo que la CONTRATISTA cuente con la autorización escrita del CONTRATANTE.

Todos los informes, especificaciones, estudios técnicos, y, en general, todos los documentos que la CONTRATISTA elabore en virtud del presente contrato, serán de propiedad exclusiva del CONTRATANTE.

La CONTRATISTA defenderá, indemnizará y mantendrá a salvo al CONTRATANTE y a sus funcionarios de y en contra de cualquier reclamación, acción, demanda, y procedimiento legal y de toda responsabilidad, daño, pérdida, juicio, declaración autorizada, costos y gastos directos e indirectos incluyendo, sin limitación, los honorarios razonables de los abogados, que surjan de o en relación con cualquier violación y/o usurpación efectuada por la CONTRATISTA de cualquier derecho de autor, patente, marca registrada, secreto industrial u otro derecho propietario o de propiedad intelectual de cualquier tercero.

5. Vendor lock-in

Los estándares empleados por los servicios contratados en virtud del presente contrato deberán permitir que el CONTRATANTE pueda recuperar y descargar los datos que se encuentran en las dependencias o sistemas del CONTRATISTA o sus subcontratistas. Ello con miras a que el CONTRATANTE pueda, sin mayores costos, migrar su información a un nuevo proveedor una vez terminado el objeto del presente contrato.

6. Fuerza mayor o caso fortuito.

Si se presentase una situación de fuerza mayor o caso fortuito en los términos que se encuentra definido por el artículo 30 del Código Civil, la CONTRATISTA deberá notificar al CONTRATANTE inmediatamente y por escrito de dicha situación y sus causas, quedando excusada de cumplir las obligaciones que emanen del presente

Contrato, desde el momento de la ocurrencia de la fuerza mayor o caso fortuito hasta la desaparición de la misma.

Si la situación de fuerza mayor o caso fortuito, se prolongase más allá de lo razonable o previsible, según la naturaleza del bien o servicio comprendido en el Contrato, o fuere evidente que éste ya no podrá cumplirse, el CONTRATANTE estará facultado para resolver el Contrato, conforme las normas de la legislación vigente.

Sin perjuicio de lo anterior, en ningún caso se considerará caso fortuito o causal de fuerza mayor lo siguiente:

(a) El embargo de los bienes del CONTRATISTA.

(b) Las acciones que pueda ordenar la autoridad que impidan al CONTRATISTA desarrollar su labor por no cumplir con las disposiciones legales o reglamentarias que le correspondan.

(c) La huelga de los trabajadores del CONTRATISTA o de alguno de sus contratistas o subcontratistas.

7. Facultad de la CONTRATANTE de comunicar el incumplimiento del CONTRATISTA a otras entidades públicas.

En caso de incumplimiento total o parcial del presente contrato por parte del CONTRATISTA, el CONTRATANTE podrá comunicar de esta circunstancia a las demás entidades de la Administración Publica que hayan contratado a éste. Asimismo, el CONTRATANTE será libre de comunicar a los demás órganos de la Administración Pública su opinión acerca de la calidad de los servicios prestados en virtud del presente contrato.

Lo anterior es sin perjuicio de las cláusulas del presente instrumento que se refieran la resolución del contrato, multas, responsabilidad civil y demás que fueren procedentes.

8. Legislación aplicable y resolución de controversias.

El presente Contrato se rige por las leyes y normas jurídicas de la República del Ecuador. Ante cualquier dificultad que se suscite entre las partes de este contrato respecto de la existencia, validez, exigibilidad, resolución, término, interpretación,

aplicación, cumplimiento o suscripción del mismo o por cualquier otra razón relacionada con este contrato, las Partes se someterán a la jurisdicción y competencia de los tribunales ordinarios de justicia de la ciudad de Quito.

9. ***Procedimiento para hacer efectiva la terminación y medidas para mantener la continuidad del servicio.***

La terminación del Contrato se efectuará por vía administrativa, sin necesidad de pronunciamiento judicial, cuando la CONTRATANTE considerare que se cumple con las causales que se establecen en el acápite [indicar cláusulas donde se establecen las causales de terminación].

La terminación del Contrato será notificada por carta certificada dirigida al domicilio indicado por la CONTRATISTA en el Contrato y se entenderá practicada a contar del tercer día hábil siguiente a su ingreso para despacho en oficina de correos.

La resolución que declara la terminación del Contrato deberá invocar la causal de terminación que se emplea, sus fundamentos, el alcance de la terminación y la fecha a contar de la cual ésta entrará en vigor.

Una vez notificado, la CONTRATISTA dispondrá de un plazo de cinco días hábiles a contar de la fecha de la comunicación para formular descargos respecto de la resolución que declara la terminación del Contrato.

Para lo anterior, la CONTRATISTA podrá acompañar todos los antecedentes que estime pertinentes.

Transcurrido este plazo, y recibido los descargos, la CONTRATANTE resolverá sobre el particular mediante resolución o resoluciones fundadas, previa ponderación de los antecedentes, remitiéndose copia del acto administrativo al CONTRATISTA.

Si transcurrido el plazo, y no habiéndose recibido descargos, o habiéndose recibido descargos, y la CONTRATANTE los hubiere rechazado, la resolución que declara la terminación del Contrato quedará a firme.

Una vez ocurrido lo anterior, la CONTRATISTA deberá entregar a la CONTRATANTE la información utilizada en la prestación de los servicios hasta ese momento, de modo de habilitar cualquier solución que este defina.

Durante el periodo que media entre la notificación de la terminación y la fecha en que se ésta se hará efectiva, la CONTRATISTA deberá prestar, a su costa, toda la

colaboración que la CONTRATANTE le requiera para que este último pueda traspasar a otro proveedor la operación del servicio de manera tal que se mantenga la continuidad del mismo en todo momento.

Adicionalmente, se podrán aplicar todas las medidas tendientes a mantener la continuidad de servicio que deba efectuar la CONTRATANTE, por cuenta, costo y riesgo del CONTRATISTA, previa notificación al mismo. Para estos efectos, a modo ejemplar, se entenderán como medidas correctivas, el tener que recurrir para la ejecución de las obligaciones contractuales del CONTRATISTA a la contratación de terceros o a funcionarios de la CONTRATANTE

ANEXO 5: VULNERABILIDADES

De acuerdo al informe “Beneficios, riesgos y recomendaciones para la seguridad de la información” de la ENISA [19] se identifican las siguientes vulnerabilidades, mismas que han sido adaptadas a la realidad del estado ecuatoriano, caso de estudio.

- ***Aplicación deficiente de las definiciones de funciones***.- En el proveedor en nube, una separación inadecuada de funciones puede conducir a roles excesivamente privilegiados que pueden convertir a los sistemas muy grandes en vulnerables. Por ejemplo, ninguna persona debería tener privilegios de acceso a toda la nube.
- ***Aplicaciones inter-nube que crean dependencia oculta***.- En la cadena de suministro existen dependencias ocultas y la arquitectura del proveedor en nube no ofrece operaciones continuas desde la nube cuando las terceras partes implicadas han sido separadas del proveedor del servicio y viceversa.
- ***Auditoría o certificación no disponible para los clientes***.- El proveedor en nube no puede ofrecer ninguna garantía al cliente vía una certificación de auditoría. Ya que por ejemplo, pueden estar utilizando hipervisores de código abierto o versiones adaptadas de los mismos (Xen), que no han alcanzado ninguna certificación de criterio común, lo que constituye un requisito fundamental para algunas organizaciones.
- ***Ausencia de aislamiento de los recursos***.- El uso de recursos por un cliente puede afectar al uso de recursos de otro, especialmente en infraestructuras IaaS, donde los recursos físicos se comparten entre múltiples equipos virtuales, y por tanto, múltiples clientes. Los hipervisores utilizados en IaaS ofrecen API integradas, que el proveedor en nube utiliza para desarrollar una interfaz de gestión de la propiedad, de provisión y de información que está expuesta a sus clientes. Las vulnerabilidades en el modelo de seguridad del hipervisor pueden llevar a un acceso no autorizado a la información del cliente. Al mismo tiempo, una vulnerabilidad en este nivel puede permitir a un atacante manipular los recursos de una instalación en nube, provocando una denegación de servicio (por ejemplo, apagado de equipos virtuales en ejecución), fuga de datos (por ejemplo, la copia y la

transferencia fuera de la nube de equipos virtuales), datos comprometidos (por ejemplo, reemplazo de equipos virtuales con copias modificadas) o daños financiero directos (por ejemplo, réplica y ejecución de numerosas copias de los equipos virtuales). Por último, la falta de herramientas para hacer cumplir un término de servicio (ToS) o un Acuerdo de nivel de servicio (SLA) más específico, como la calidad de servicio (CdS) o los productos de planificación de recursos distribuidos (DRS) podrían permitir a un cliente monopolizar el uso de la nube, con impactos a otros clientes en forma de denegación de servicio o rendimiento pobre.

- ***Ausencia de conciencia de seguridad***.- Los clientes en nube no son conscientes de los riesgos que podrían afrontar al migrar hacia la nube, en particular aquellos riesgos generados a partir de amenazas específicas de la nube, es decir, pérdida de control, cierre de la empresa proveedora, agotamiento de recursos del proveedor en nube, etc. Esta falta de conciencia también podría afectar al proveedor en nube, que puede no ser consciente de las medidas que debería tomar para mitigar estos riesgos.
- ***Ausencia de políticas de limitación de recursos***.- Si no existe un modo flexible y configurable para que el cliente y/o el proveedor en nube establezcan límites sobre los recursos, puede haber problemas cuando el uso de recursos sea impredecible.
- ***Cláusulas SLA que contienen un riesgo de negocio excesivo***.- Los SLA pueden acarrear demasiado riesgo de negocio para un proveedor, dado el riesgo real de fallos técnicos. Desde el punto de vista del cliente, los SLA pueden contener cláusulas que resulten ser perjudiciales; por ejemplo, en el terreno de la propiedad intelectual, un SLA puede especificar que el proveedor en nube posee los derechos de cualquier material almacenado en la infraestructura en nube.
- ***Falta de aislamiento de la reputación***.- Las actividades de un cliente pueden afectar a la reputación de otro cliente.
- ***Falta de control en el proceso de evaluación de vulnerabilidad***.- Las restricciones al escaneado de puertos y los tests de vulnerabilidad son una vulnerabilidad importante que, en combinación con una condición de uso que

haga responsable al cliente de asegurar los elementos de la infraestructura, constituye un problema grave de seguridad.

- ***Falta de tecnologías y soluciones estándar.-*** Una falta de medios estándar significa que los datos pueden estar ligados a un proveedor. Es un riesgo importante si el proveedor cesa sus operaciones. Esto puede frenar el uso de servicios de gestión de seguridad y tecnologías de seguridad externa como la gestión federada de la identidad (FIM).
- ***Funciones y responsabilidades confusas***.- Estas vulnerabilidades se refieren a la atribución inadecuada de funciones y responsabilidades en la organización del proveedor en nube.
- ***Imposibilidad de procesar datos codificados***.- La codificación de datos estáticos no es difícil, pero a pesar de los avances recientes en codificación homomórfica no hay indicios de un sistema comercial capaz de mantener esta codificación durante el procesamiento
- ***Modelado inadecuado del uso de recursos***.- Los servicios en nube son particularmente vulnerables al agotamiento de recursos debido a que no se provisionan estadísticamente. Aunque muchos proveedores permiten que los clientes reserven recursos con antelación, los algoritmos de provisión de recursos pueden fallar.
- ***No aplicación del principio de «Need-to-Know»***.- Éste es un tipo especial de vulnerabilidad relativa a los roles y las responsabilidades. No debería darse un acceso a los datos innecesarios a las partes. De otro modo, ello constituye un riesgo innecesario.
- ***Posibilidad de que se realice un análisis interno de la red (en Nube)***.- Los clientes en nube pueden llevar a cabo escaneados de puertos y otras pruebas en otros clientes dentro de la red interna.
- ***Posibilidad de que se realicen comprobaciones de corresidencia***.- Los ataques por vía alternativa que aprovechan una falta de aislamiento de los recursos permiten a los atacantes determinar qué recursos están compartidos por qué clientes.
- ***Procedimientos de seguridad física inadecuados***.- Vulnerabilidad relacionada con la falta de controles sobre el perímetro físico (tarjeta

inteligente de autenticación en la entrada) o la falta de escudo electromagnético para los activos críticos vulnerables a escuchas.

- ***Sincronización de las responsabilidades o las obligaciones contractuales externas a la Nube***.- Frecuentemente, los clientes en nube no son conscientes de las responsabilidades que asumen en las condiciones de servicio. Hay una tendencia a atribuir erróneamente al proveedor en nube la responsabilidad de actividades como la codificación de archivos, incluso aunque esté claramente señalado en los términos del contrato entre las dos partes que no se ha asumido ninguna responsabilidad de ese tipo.
- ***Sistemas de certificación no adaptados a las infraestructuras de nube***.- En el mercado ecuatoriano hasta la presente no existe ningún control específico de nube, lo que quiere decir que las vulnerabilidades de seguridad probablemente pasarán desapercibidas.
- ***Vulnerabilidades AAA***.- Un sistema pobre de autenticación, autorización y auditoría podría facilitar el acceso no autorizado a recursos, el aumento de privilegios, la imposibilidad de rastrear el uso indebido de recursos y de incidentes de seguridad en general. Además, la nube hace que los ataques de autenticación basados en contraseñas (práctica fraudulenta que utiliza un troyano para robar contraseñas corporativas) tengan un impacto mucho mayor, ya que las aplicaciones corporativas ahora están expuestas en Internet. Por tanto, la autenticación basada en contraseñas llegará a ser insuficiente y será necesaria una autenticación más robusta o de dos factores para acceder a los recursos en nube.
- ***Vulnerabilidades de la aplicación o gestión de parches insuficiente***.- Esta clase de vulnerabilidades incluye: errores en el código de la aplicación, procedimientos de parcheado conflictivos entre el proveedor y el cliente, aplicación de parches no examinados, vulnerabilidades en los navegadores.
- ***Vulnerabilidades del hipervisor.-*** Los ataques a la capa del hipervisor son muy atractivos: el hipervisor, de hecho, controla totalmente los recursos físicos y los equipos virtuales que se ejecutan sobre él, así que cualquier vulnerabilidad en esta capa es extremadamente crítica. Explotar una

vulnerabilidad del hipervisor equivale potencialmente a explotar todos los equipos virtuales.