



**GUÍA DE AUDITORÍA PARA EVALUAR EL ASEGURAMIENTO DE LA  
DISPONIBILIDAD DE LA INFORMACIÓN EN UN AMBIENTE CLOUD  
COMPUTING IAAS, BAJO LA NORMA ISO 27001 DE 2013**

**CRISTIAN GIOVANNY TORO SÁNCHEZ  
JOHAN SEBASTIÁN MURCIA PRIETO  
MARIEN HERNÁNDEZ VEGA**

**UNIVERSIDAD CATÓLICA DE COLOMBIA  
FACULTAD DE INGENIERÍA  
PROGRAMA DE ESPECIALIZACIÓN EN AUDITORÍA DE SISTEMAS DE  
INFORMACIÓN  
BOGOTÁ D.C.  
2014**

**GUÍA DE AUDITORÍA PARA EVALUAR EL ASEGURAMIENTO DE LA  
DISPONIBILIDAD DE LA INFORMACIÓN EN UN AMBIENTE CLOUD  
COMPUTING IAAS, BAJO LA NORMA ISO 27001 DE 2013**


**CRISTIAN GIOVANNI TORO SÁNCHEZ  
JOHAN SEBASTIÁN MURCIA PRIETO  
MARIEN HERNÁNDEZ VEGA**

**Trabajo de Grado**

**Director  
HOLMAN DIEGO BOLÍVAR BARÓN  
Ingeniero de Sistemas**

**UNIVERSIDAD CATÓLICA DE COLOMBIA  
FACULTAD DE INGENIERÍA  
PROGRAMA DE ESPECIALIZACIÓN EN AUDITORÍA DE SISTEMAS DE  
INFORMACIÓN  
BOGOTÁ D.C.  
2014**

## TIPO DE LICENCIA




### Atribución-NoComercial 2.5 Colombia (CC BY-NC 2.5 CO)

Este es un resumen legible por humanos (y no un sustituto) de la [licencia](#).

[Advertencia](#)


**Usted es libre para:**




- Compartir — copiar y redistribuir el material en cualquier medio o formato
- Adaptar — remezclar, transformar y crear a partir del material

El licenciante no puede revocar estas libertades en tanto usted siga los términos de la licencia

**Bajo los siguientes términos:**



Atribución — You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.



NoComercial — Usted no puede hacer uso del material con  fines comerciales .

No hay restricciones adicionales — Usted no puede aplicar términos legales ni medidas tecnológicas que restrinjan legalmente a otros hacer cualquier uso permitido por la licencia.

2

## **Nota de aceptación**

Aprobado por el comité de grado en cumplimiento de los requisitos exigidos por la Facultad de Ingeniería y la Universidad Católica de Colombia para optar al título de ingenieros de Sistemas.

---

Ingeniero Holman Diego Bolívar  
Director

---

Ingeniero Holman Diego Bolívar  
Revisor Metodológico

Bogotá D. C. 6 de Diciembre de 2014.

*A nuestras familias,  
por su apoyo permanente  
e incondicional.*

## **AGRADECIMIENTOS**

Agradecemos primeramente a Dios por las bendiciones recibidas y por permitirnos compartir esta experiencia de vida; a nuestros padres quienes han sido nuestros precursores y quienes nos encaminaron por el sendero del conocimiento; a nuestras esposas y esposos por su amor, paciencia y apoyo incondicional; a nuestros hijos e hijas por ceder el tiempo de juegos y apapachos.

Agradecemos a nuestros maestros porque nunca dijeron no, porque aclararon cualquier duda o incertidumbre, porque con su paciencia y dedicación lograron hacer de nosotros grandes personas y excelentes profesionales; a la Universidad Católica de Colombia por su intensa formación en valores y por acogernos como en casa.

## CONTENIDO

	Pág.
INTRODUCCIÓN	15
1. PLANTEAMIENTO DEL PROBLEMA	16
1.1. EL TAMAÑO DEL MERCADO DE CLOUD COMPUTING – 2013	16
1.2. PROYECCIÓN DE GANANCIAS DE AMAZON.COM - 2014	16
1.3. LAS EMPRESAS SE MUEVEN HACIA LA NUBE.	17
1.4. LA SEGURIDAD COMO SU PRINCIPAL PREOCUPACIÓN PARA LA TRANSICIÓN A LA NUBE	18
1.5. LAS CARGAS DE TRABAJO DE SERVIDOR QUE ESTARÁN VIRTUALIZADOS EN 2014	19
2. OBJETIVOS DEL PROYECTO	23
2.1. OBJETIVO GENERAL	23
2.2. OBJETIVOS ESPECÍFICOS	23
3. ESTADO DEL ARTE	24
3.1. HISTORIA DEL CONCEPTO NUBE	24
3.2. COMPUTACIÓN GRID	25
3.3. GOOGLE FILE SYSTEM	26
3.4. CLOUD COMPUTING EN LOS ÚLTIMOS AÑOS	27
3.5. TIPOS DE NUBE	28
3.5.1. Nubes Públicas.	28
3.5.2. Nubes Privadas.	28
3.5.3. Nubes Híbridas.	28
3.6. CLOUD COMPUTING	28
3.6.1. Cloud Software as a Service (saas).	29
3.6.2. Cloud Platform as a Service (paas).	30
3.6.3. Cloud Infrastructure as a Service (iaas).	33

3.7. CASOS DE ÉXITO DE COMPUTACIÓN EN LA NUBE	35
3.7.1. Avanxo.	35
3.7.2. Novartis.	36
3.7.3. Avantel - gmail transforma las comunicaciones.	36
3.7.4. Fedepalma del correo a la colaboración.	37
3.8. SEGURIDAD DE LA INFORMACIÓN	37
3.9. ACUERDOS DE NIVEL DE SERVICIO	41
3.9.1. Qué es un ans.	41
3.9.2. Qué es un ons.	42
3.9.3. Monitoreo y medición.	42
3.9.4. Factores deberían considerarse en los términos del sla.10	42
3.9.5. Requisitos del ans.	44
3.10. CLASIFICACIÓN TIER EN EL DATACENTER.	46
3.10.1. TIER I: centro de datos básico.	47
3.10.2. TIER II: centro de datos redundante.	47
3.10.3. TIER III: centro de datos concurrentemente mantenibles.	48
3.10.4. TIER IV: centro de datos tolerante a fallos.	48
3.10.5. Estándares en los data center.	48
3.11. MARCO GUÍA DE AUDITORÍA	49
4. METODOLOGÍA PROPUESTA	51
4.1. ALCANCE DE LA GUÍA DE AUDITORÍA	51
4.2. SECTORES Y ÁREAS DE APLICACIÓN DE LA GUÍA DE AUDITORÍA	51
4.3. ANÁLISIS DE RIESGOS	52
4.4. PARTES INTERESADAS	53
5. CARACTERIZACIÓN DE DOMINIOS NORMA ISO 27001	54
6. ESTRUCTURACIÓN DE LA GUÍA DE AUDITORÍA	55
7. VALIDACIÓN DE GUÍA DE AUDITORÍA	56
8. CONCLUSIONES	57
BIBLIOGRAFÍA	58



## LISTA DE FIGURAS

FIGURA 1. PUNTUACIÓN GLOBAL DE COMPUTACIÓN EN NUBE DE BSA 2013	18
FIGURA 2. TENDENCIAS DE ADOPCIÓN DE CLOUD COMPUTING EN COLOMBIA 2013	20
FIGURA 3. MODELO CLOUD COMPUTING	34
FIGURA 4. NIVELES TIER EN DATACENTER	47
FIGURA 5. ESTÁNDARES DE LOS DATACENTER	49

## LISTA DE ANEXOS

	<b>Pág.</b>
ANEXO A - CARACTERIZACIÓN DE LA NORMA ISO 27001	60
ANEXO B - GUÍA DE AUDITORÍA PARA EVALUAR EL ASEGURAMIENTO DE LA DISPONIBILIDAD EN UN AMBIENTE CLOUD COMPUTING IAAS BAJO LA NORMA ISO 27001 DE 2013	61
ANEXO C - CARTA INVITACIÓN A EVALUACIÓN DE GUÍA	62
ANEXO D - VALIDACIÓN DE LA GUÍA DE AUDITORIA PARA EVALUAR EL ASEGURAMIENTO DE LA DISPONIBILIDAD EN UN AMBIENTE CLOUD COMPUTING IAAS BAJO LA NORMA ISO 27001 DE 2013	63

## GLOSARIO

**AUDITAR:** Es una actividad informática que requiere un determinado desempeño profesional para cumplir unos objetivos precisos.

**AUDITORÍA:** Es un control selectivo, efectuado por un grupo independiente del sistema a auditar, con el objetivo de obtener información suficiente para evaluar el funcionamiento del sistema bajo análisis.

**AUDITORÍA DE SISTEMAS:** Métodos de evaluación a los procesos, procedimientos, normas o leyes que se usan en los sistemas de control interno informático; verificando a través de una evidencia el estado de los controles de los sistemas informáticos.

**AUDITORÍA EXTERNA:** Es aquella que es realizada por personas ajenas a la empresa auditada, debidamente calificada que cumple con estándares y mitologías.

**AUDITORÍA INTERNA:** Es aquella que es realizada con recursos materiales y personas que pertenecen a la Empresa auditada. Cuenta con un proceso metodológico bajo un plan interno de auditoría.

**CLOUD COMPUTING:** un modelo para habilitar un cómodo acceso en red omnipresente, a solicitud, a un conjunto compartido de recursos informáticos configurables (por ejemplo redes, servidores, recursos de almacenamiento o aplicaciones y servicios) que se pueden conformar y proveer rápidamente con un esfuerzo administrativo mínimo o una interacción mínima con el proveedor de servicios

**CONFIDENCIALIDAD:** Es aquello que se cumple cuando sólo las personas autorizadas pueden conocer los datos o la información correspondiente.

**CONTROL:** Mecanismo o acción implementada, que ayuda a disminuir la probabilidad de impacto de que se materialice un riesgo.

**CONTROL CORRECTIVO:** Los controles Detectivos registran un evento después de que este ha sucedido

**CONTROL DETECTIVO:** Los controles Detectivos registran un evento después de que este ha sucedido

**CONTROL PREVENTIVO:** Los Controles Preventivos detienen que un evento suceda.

**DISPONIBILIDAD:** Es aquello que se alcanza si las personas autorizadas pueden acceder a tiempo a la información a la que estén autorizadas; la continuidad en el servicio y en las operaciones en el ahora y en el futuro.

**EVALUACIÓN:** Es el proceso de recolección y análisis de información, y a partir de ella presentar las recomendaciones que facilitarán la toma de decisiones.

**EVALUACIÓN DE RIESGO:** Es el proceso utilizado para identificar y evaluar riesgos y su impacto potencial.

**EVIDENCIA:** Es toda información que utiliza el auditor para determinar si el ente o los datos auditados siguen los criterios u objetivos de la auditoría.

**IAAS:** El concepto de Infraestructura como Servicio (IaaS, Infrastructure as a Service) es uno de los tres modelos fundamentales en el campo del cloud computing, junto con el de Plataforma como Servicio (PaaS, Platform as a Service) y el de Software como Servicio (SaaS, Software as a Service). Al igual que todos los servicios cloud, IaaS proporciona acceso a recursos informáticos situados en un entorno virtualizado, la "nube" (cloud), a través de una conexión pública, que suele ser internet.

**INFORME DETALLADO:** Informe de auditoría dirigido al usuario, en lenguaje técnico, contiene al detalle todas las recomendaciones que se pueden materializar vs el criterio del auditor.

**INFORME GERENCIAL:** Dirigido a la alta gerencia y al jefe de informática, concreto, con las principales recomendaciones y puntos mejorables, en un lenguaje bajo en tecnicismos y no mayor a 3 hojas.

**INFRAESTRUCTURA TECNOLÓGICA:** Conjunto de elementos hardware y software donde se asientan los diferentes servicios que se consideran necesarios para el funcionamiento de una organización o para el desarrollo de una actividad.

**INTEGRIDAD:** Consiste en que sólo los usuarios autorizados puedan variar los datos; veracidad de la información o la completitud y exactitud de la información o los datos.

**PAAS:** es una categoría de servicios cloud que proporciona una plataforma y un entorno que permiten a los desarrolladores crear aplicaciones y servicios que funcionen a través de internet.

**PRIVACIDAD:** Mecanismos definidos para proteger y garantizar la confidencialidad de los datos.

**REDES:** Estructura física y lógica para interconectar equipos con el propósito de compartir recursos tecnológicos.

**RESUMEN EJECUTIVO:** Es un informe de fácil lectura, gramaticalmente correcto y breve que presenta los hallazgos a la gerencia en forma comprensible.

**RIESGO:** Es la posibilidad de que ocurra un hecho o suceso que pueda tener efecto adverso sobre la organización y sus sistemas de información.

**RIESGO DE CONTROL:** Es el riesgo que los sistemas de control en vigencia no puedan detectar o evitar errores o irregularidades significativas en forma oportuna.

**RIESGO DE DETECCIÓN:** Es el riesgo que a través de la labor de auditoría no se detecten errores o irregularidades significativas en el caso que existiesen y no hubiesen sido prevenidos o detectados por los sistemas de control.

**RIESGO DEL NEGOCIO:** Son aquellos riesgos que pueden afectar la viabilidad a largo plazo de un determinado negocio o de la empresa en su conjunto.

**RIESGO INHERENTE:** Es la susceptibilidad a errores o irregularidades significativas, antes de considerar la efectividad de los sistemas de control.

**SAAS:** se describe cualquier servicio cloud en el que los consumidores puedan acceder a aplicaciones de software a través de internet.

**SEGURIDAD:** Característica que indica que un sistema está libre de todo peligro, daño o riesgo.

**SEGURIDAD FÍSICA:** Conjunto de mecanismos de protección establecidos a nivel físico para proteger la infraestructura y la integridad humana.

**SEGURIDAD LÓGICA:** Conjunto de mecanismos para proteger datos programas.

## RESUMEN

En la actualidad, una de las nuevas tendencias del mercado es la proliferación de los servicios operados en la nube, los cuales permiten la asignación dinámica de recursos en función de las necesidades de los usuarios, ya que tienen como beneficio la reducción de costos en infraestructuras y mayor disponibilidad de acceso a los recursos o servicios. Sin embargo con la adopción de estos nuevos modelos basados en los ambientes en nube, surgen nuevos retos para la auditoría de sistema como la evaluación y creación de controles que permitan la gestión de riesgos y que garanticen la disponibilidad de la información de manera íntegra y confiable.

Este proyecto de grado genera como resultado una guía de auditoría para evaluar el aseguramiento de la disponibilidad de la información en un ambiente de infraestructura en la nube (Cloud Computing IaaS), bajo la norma ISO 27001 de 2013. La guía comprende un compendio de buenas prácticas en la auditoría de sistemas, que se aplican en la auditoría tradicional, pero que se adecuan o modifican para ser aplicadas en la auditoría en la nube; la finalidad de esta guía es brindar un apoyo a las organizaciones que están pensando en tomar un servicio de infraestructura en la nube o que quieren evaluar el nivel de disponibilidad de su servicio de infraestructura interno.

Para el desarrollo de esta guía se tomó como referente la norma ISO 19011 de 2012 y otras buenas prácticas en la auditoría para estructurar el contenido de la guía; luego se evaluaron los dominios de la norma ISO 27001 de 2013 bajo tres criterios (comunicaciones, continuidad y nivel de servicio) con el objetivo de filtrar los más relevantes al momento de evaluar la disponibilidad de la información.

Finalmente, un grupo de expertos en auditoría validó la guía y sus formatos, obteniendo como resultado un documento de apoyo para la realización de cualquier auditoría, cuya finalidad sea evaluar el aseguramiento de la disponibilidad de la información.

**Palabras Clave:** auditoría de información, infraestructura, computación en la nube.

## **ABSTRACT**

Today, one of the new market trends is the proliferation of operated services in the cloud, which allows dynamic allocation of resources according to the needs of the users, since they have the benefit of reducing infrastructure costs increased availability and access to resources or services. However, with the adoption of these new models based on cloud environments, new challenges arise for the audit of the system as the evaluation and development of controls that enables the management of the risk and guarantee that the data be available and reliable.

The result of the degree project is generated an audit guide to evaluate the availability of the data on a cloud infrastructure (IaaS Cloud Computing) under the ISO 270001 standard 2013. The guide includes a compendium of good practices in auditing systems, which are applied in traditional audit, but modified to fit or be applied in the audit in the cloud; The purpose of this guide is to provide support to organizations that are thought of taking service cloud infrastructure or want to assess the level of availability of its own internal infrastructure.

For the development of this guide I took as a reference to ISO 19011, 2011 and other good practices in the audit to structure the content of the guide; then the domain of ISO 27001 2013 standard under three criteria (communication, continuity and service level) in order to filter the most relevant when assessing the availability of the information is evaluated.

Finally, an expert auditor group validate the audit guide and formats, resulting in a support document for the conduct of any audit, whose purpose is to evaluate the assurance of the availability of information.

**Key Words:** audit information, infrastructure, cloud computing

## **INTRODUCCIÓN**

Debido al cambiante mundo tecnológico y la incorporación de alternativas virtuales para el almacenamiento de la información y de la provisión de servicios de TIC a través de la nube (procesamiento y almacenamiento masivo de datos en servidores que alojen la información del usuario) y contemplando los riesgos que en este entorno se pueden generar, este trabajo de investigación pretende analizar las buenas prácticas que usa la función auditora y la gestión de la seguridad de la información para cumplir con la correcta evaluación de los controles que garantizan el aseguramiento de la disponibilidad de la información en la nube.

Basado en este precedente nos proponemos desarrollar una guía de auditoría, para poderla aplicar en la auditoría de sistemas en la nube, a partir de la identificación y análisis de buenas prácticas como la norma ISO 27001 de 2013 y así de esta forma evaluar uno de los criterios de información que satisfacen los objetivos de un negocio, como lo es la disponibilidad de la información.



## **1. PLANTEAMIENTO DEL PROBLEMA**

En la actualidad una de las nuevas tendencias del mercado es la proliferación de los servicios operados en la nube, los cuales permiten la asignación dinámica de recursos en función de necesidades de los clientes, ya que tienen como beneficio la reducción de costos en infraestructuras y mayor disponibilidad de acceso a los recursos o servicios.

¿Cuáles son las buenas prácticas en la auditoría de sistemas, para evaluar el aseguramiento de la disponibilidad de la información en la computación en la nube?

Un informe presentado por la compañía SONDA, una de las principales empresas latinoamericanas en incorporar servicios cloud, expone las siguientes cinco estadísticas<sup>1</sup> las cuales ilustran un poco el panorama actual de la computación en la nube.

### **1.1. EL TAMAÑO DEL MERCADO DE CLOUD COMPUTING – 2013**

Este es un estudio realizado por Gartner donde afirma que en \$ 150 mil millones crecerá el tamaño del mercado de Cloud Computing en - 2013.

Esta cantidad proviene de un estudio realizado por Gartner. El número puede parecer una estimación alta para algunos, pero es consistente (o baja) en comparación con otras estimaciones. La investigación de Merrill Lynch predice que el mercado de cloud computing para un valor de \$ 160 mil millones para el mismo año. Con muchas empresas apenas empezamos a sentir la presión para pasar a la computación en nube, no es de extrañar que los expertos predigan que el mercado crezca a una tasa tan alta en los próximos años.

### **1.2. PROYECCIÓN DE GANANCIAS DE AMAZON.COM - 2014**

Amazon publicó un reporte financiero del segundo trimestre del 2014. Según la información compartida, el valor de las acciones de la compañía cayó \$0.27 USD por unidad, lo que resultó inquietante para algunos accionistas, ya que los analistas esperaban que la pérdida rondara \$0.15 USD. Amazon reveló ingresos por \$19.24 mil MDD (Millones de dólares), lo que representa un crecimiento de 23% con relación con el mismo período del año pasado.

---

<sup>1</sup> SONDA Cloud Computing, Informes Digitales [en línea]. [citado 24 julio 2014]. Disponible en internet: <<http://cloudempresarial.com/tweets/5-estadisticas-del-cloudcomputing-que-usted-puede-encontrar-sorprendentes/>>

Cabe señalar que las pérdidas netas durante el trimestre fueron \$126 MDD, un aumento significativo si se tiene en cuenta que éstas fueron \$7 MDD durante el mismo lapso de 2013. Las malas noticias causaron que el valor de la compañía cayera 5% en el transcurso de las operaciones ordinarias de la bolsa. Un detalle interesante es que la empresa aumentó considerablemente sus gastos operativos, especialmente por la contratación de miles de empleados nuevos durante 2013.

De cualquier manera, representantes de la compañía revelaron que esperan recibir ingresos entre \$19.7 mil MDD y \$21.5 mil MDD y pérdidas que oscilan entre \$820 MDD y \$410 MDD durante el tercer trimestre del año, por lo que el panorama seguirá siendo oscuro para sus accionistas. Aparentemente, los directivos culpan de la situación al proceso de amortización de bienes intangibles y a un programa de compensaciones por acción de una buena parte de las pérdidas operativas que se prevén para el siguiente trimestre.

Lo anterior genera un punto de reflexión adicional; no es solo saber si las acciones suben o bajan y la pérdida se refleje en las acciones, sino, que el mercado de los servicios ofrecidos en la nube ahora son mas diversos y otras empresas granan mayores clientes opacando a Amazon.

### **1.3. LAS EMPRESAS SE MUEVEN HACIA LA NUBE.**

7 de cada 10 empresas que utilizan servicios en la nube, se mueven a nuevas aplicaciones a la nube.

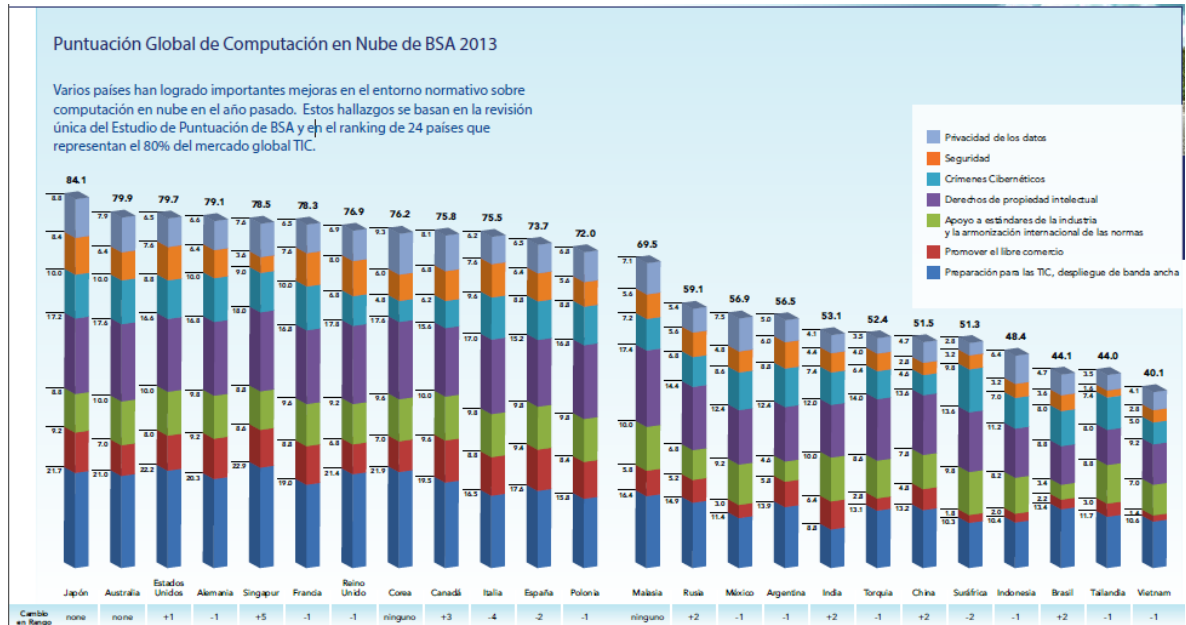
Esta estadística está basada en un estudio realizado por Mímicas, una empresa que ofrece software como una empresa de servicio de correo electrónico. Muchas empresas comienzan su transición a la nube con un pequeño “estudio”; para ello, sólo una parte de su infraestructura, aplicaciones o datos. Una gran parte del crecimiento de la industria en los próximos años será de las empresas que están contentos con su “período de prueba” están listos para la transición y aún más sus negocios en la nube.

Por otro lado BSA<sup>2</sup> | Te Software Alliance, es la principal defensora de la industria global de software ante los gobiernos y el mercado internacional. Es una asociación de compañías de primera clase que invierten miles de millones de dólares al año para crear soluciones de software que activen la economía y mejoren la vida. En el año 2013 realizó un informe sobre la puntuación global del cloud computing en el mundo, la siguiente figura ilustra los 24 países que representan el 80% del mercado global de TIC.

---

<sup>2</sup> BSA - The Software Alliance. Global Cloud Computing Scorecard, [en línea]. [citado 4 octubre de 2014]. Disponible en internet: [<http://cloudscorecard.bsa.org/2013/assets/PDFs/BSA\\_GlobalCloudScorecard2013\\_Spanish.pdf/>](http://cloudscorecard.bsa.org/2013/assets/PDFs/BSA_GlobalCloudScorecard2013_Spanish.pdf)

FIGURA 1. PUNTUACIÓN GLOBAL DE COMPUTACIÓN EN NUBE DE BSA 2013



Fuente: BSA - The Software Alliance<sup>3</sup>

#### 1.4. LA SEGURIDAD COMO SU PRINCIPAL PREOCUPACIÓN PARA LA TRANSICIÓN A LA NUBE

54%: Importe de los encuestados citó la seguridad como su principal preocupación para la transición a la nube.

Este número es de acuerdo a una reciente encuesta realizada por LinkedIn con 7.052 encuestados. La seguridad es un elemento disuasorio superior para muchas empresas que buscan utilizar la computación en nube en su compañía. Esto es especialmente cierto para las industrias que utilizan y almacenan datos confidenciales, como las industrias financieras y de salud. Hace unos años, este tipo de empresas nunca se le ocurriría que usar la nube sería un método seguro para almacenar todos sus datos. Sin embargo, los proveedores de cloud son ahora capaces de llegar a cumplir con las normas de seguridad múltiples, tales como HIPAA, ISO 27001 y PCI DSS. Esto permite que este tipo de industrias con datos sensibles y de alta seguridad sentirse seguros de que sus datos están seguros al utilizar la computación en nube, de hecho, en un estudio realizado por

<sup>3</sup> BSA. Estudio sobre puntuación global de computación en la nube BSA 2013. [en línea] EE.UU: BSA [citado en 12 de Agosto de 2014]. Disponible en internet: <[http://cloudscorecard.bsa.org/2013/assets/PDFs/BSA\\_GlobalCloudScorecard2013\\_Spanish.pdf](http://cloudscorecard.bsa.org/2013/assets/PDFs/BSA_GlobalCloudScorecard2013_Spanish.pdf)>

Mímicas, el 57% de los encuestados en realidad sentía que el cloud computing había aumentado su seguridad en comparación con los métodos tradicionales para la informática y los datos de copia de seguridad.

### **1.5. LAS CARGAS DE TRABAJO DE SERVIDOR QUE ESTARÁN VIRTUALIZADOS EN 2014<sup>4</sup>**

60%: las cargas de trabajo de servidor que estarán virtualizados en 2014.

Esta predicción viene de la investigación llevada a cabo por Gartner. Este es un porcentaje impresionante, especialmente en comparación con 2008, cuando sólo el 12% de cargas de trabajo fueron virtualizados. Un negocio de la virtualización de su carga de trabajo en las nubes tiene múltiples beneficios. En primer lugar, se están ahorrando la molestia de tener que comprar y almacenar hardware físico, que es costoso e ineficiente. En segundo lugar, las empresas pueden reducir su huella de carbono mediante la subcontratación de su carga de trabajo para centros de datos, nuevos centros de datos del estado de la técnica de los equipos y procedimientos para reducir el consumo. Esto es especialmente importante cuando se consideran todos los procesos de uso intensivo de energía de un centro de datos lleva a cabo, como la refrigeración de los servidores y mantenerlos en funcionamiento 24 / 7. Por lo tanto, utilizando los centros de datos verdes es más ecológico que la vivienda de sus propios servidores.

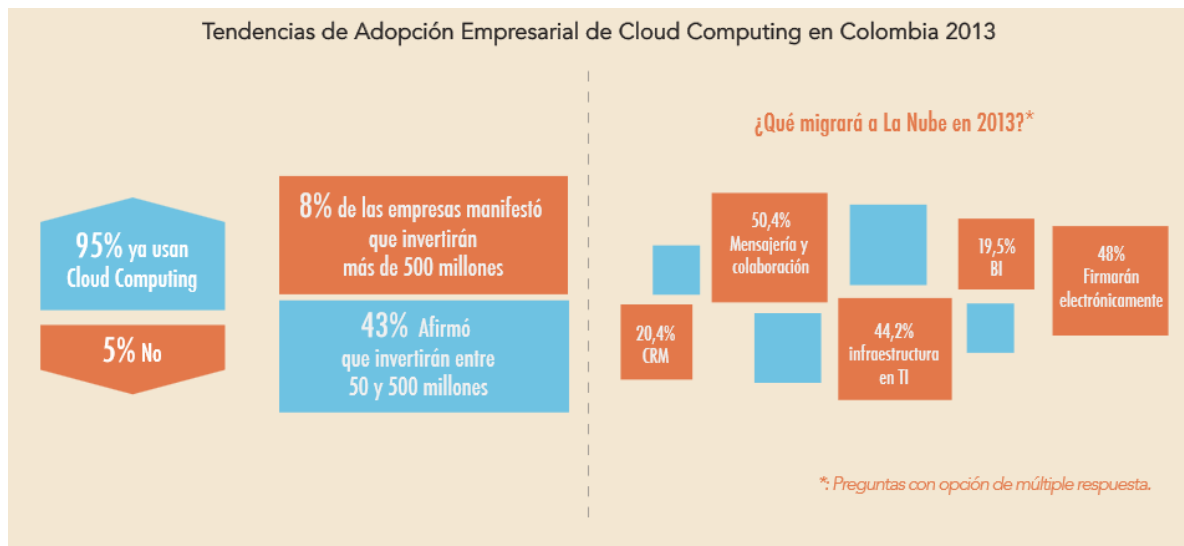
En otros estudios publicado por CINTEL hacen referencia a la incorporación empresarial de ambientes cloud computing en Colombia, enmarcado en el primer estudio nacional de tendencias Cloud Computing en el país.

Avanxo y Position Comunicaciones publicaron la segunda edición de este estudio que incorpora varios aspectos de las tendencias de las compañías más grandes y representativas del país, en cuanto a su adopción de tecnologías en la nube y redes sociales, cubriendo temas como el grado de adopción actual, la disposición de las compañías a invertir en este tipo de tecnologías en 2013, el presupuesto a destinar en ellas este año y el criterio de selección de sus proveedores.

---

<sup>4</sup> BSA - The Software Alliance. Global Cloud Computing Scorecard, [en línea]. [citado 4 octubre de 2014]. Disponible en internet en internet: <<http://www.cloudempresarial.com/tweets/5-estadisticas-del-cloudcomputing-que-usted-puede-encontrar-sorprendentes/>>

FIGURA 2. TENDENCIAS DE ADOPCIÓN DE CLOUD COMPUTING EN COLOMBIA 2013



Fuente: CINTEL. Nuevas tecnologías<sup>5</sup>

En la figura se muestra que el 95% de las empresas más grandes y representativas del país ya utilizan cloud computing.

Sólo 5% se abstendrá a la nube en 2013.

El sector con el mayor nivel de adopción de la nube es consumo masivo y los sectores con menor nivel de adopción son industria y gobierno, pero en general hay un nivel bastante elevado de adopción del cloud computing como modelo de consumo de tecnología por parte de las empresas más grandes a través de los distintos sectores de la economía nacional.

De acuerdo con el estudio, solamente el 5% de las empresas más grandes del país no está contemplando migrar a la nube soluciones de negocio en 2013, mejorando en un punto la cifra publicada en 2012 respecto a la adopción de tecnologías cloud, lo que indicaría un leve aumento en la adopción por parte de los llamados “rezagados” (Lagares); un término acuñado por Everett Rogers en la teoría de difusión de las innovaciones para definir a los más tímidos en términos de adopción de tecnología e innovación.

Otro punto importante del estudio es la selección del proveedor que presta los servicios de cloud; Recursos locales expertos en el cloud computing (profesionales

<sup>5</sup> CINTEL. Centro de Investigación y Desarrollo en Tecnologías de la Información y las Comunicaciones [en línea]. [citado 4 octubre de 2014]. Disponible en internet: <<http://cintel.org.co/wp-content/uploads/2013/06/resultados-del-estudio.pdf>>

en el país expertos en cloud computing). Más del 70% de los encuestados coincidió en que lo más relevante al momento de elegir un proveedor cloud es que tenga recursos expertos en Colombia y presente casos de éxito en empresas del país.

Ambientados en este marco referencial, es donde se plantea que con la adopción de estos nuevos modelos empresariales basados en los ambientes Cloud, surgen nuevos retos para otras áreas relacionadas con las TIC (Tecnologías de información y comunicación), como la gestión y ejecución de la auditoría de sistema para evaluar el estado de los controles, la validación de los riesgos gestionados por la organización y la verificación del cumplimiento de las normatividades.

Los servicios en la nube, ponen grandes ventajas en manos de los clientes; sobre todo de carácter económico. Sin embargo se debe contar con una adecuada orientación sobre gestión de los riesgos en la organización de acuerdo a los activos que se van a colocar en este tipo de servicios. Toda vez que el estándar ISO; nombra que uno de los activos más importantes de toda organización es la información y que por ellos hay que saberla gestionar.

Por tal motivo, la incursión de nuevas tecnologías que apoyen las operaciones diarias del negocio, conlleva a pensar formas adecuadas de controlar estos ambientes por medio de auditorías asegurando controles que ayuden a reducir los riesgos en el negocio, teniendo en cuenta lo nombrado en una presentación por la entidad ISACA: “No hay estándares específicamente publicados para cloud, sin embargo los estándares ya existentes pueden servir para concretar y acotar determinadas áreas de revisión”<sup>6</sup>.

Es basado en estas afirmaciones y estadísticas que antes de adquirir un servicio en la nube, se debería realizar una verificación o evaluación a los proveedores para seleccionar un adecuado servicio en la nube, que garantice la disponibilidad de la información pero de maneja integra y confiable, y así mismo generar auditoría efectivas y eficaces basadas en buenas prácticas que tengan un criterio homogéneo para una aplicabilidad en general, pero orientadas a garantizar controles efectivos que permitan mantener la información disponible en este tipo de entornos.

El planteamiento de este problema nos conlleva a realizarnos la siguiente pregunta:

---

<sup>6</sup> CSA, Security Guidance for Critical Areas of Focus in Cloud Computing V2.1 [en línea]. [citado 8 Agosto de 2014] Disponible en internet: <<http://www.cloudsecurityalliance.org/guidance/csaguide.pdf>>

**¿Cuáles son las buenas prácticas en la auditoría de sistemas, para evaluar el aseguramiento de la disponibilidad de la información en la computación en la nube?**

Teniendo en cuenta el contexto problemático en el que se desarrolla este trabajo de investigación y alrededor de la necesidad de conocer las buenas prácticas aplicadas a proteger la información en tecnologías a través de la internet, esta temática se inscribe en la línea de software inteligente y convergencia tecnológica de la Universidad Católica de Colombia, toda vez que al realizar este trabajo se podrá establecer un punto de referencia basado en buenas prácticas para aplicar una auditoría a la seguridad de la información para las tecnologías en la nube.

El resultado de esta investigación será de gran utilidad para los especialistas en auditoría, y las empresas auditoras que realizan verificación y evaluación a la efectividad de los controles informáticos, ya que los proveerá de conocimientos y mecanismos que les permitan ejecutar su labor en la nube, y para los usuarios finales que son los directamente involucrados, les proveerá una perspectiva más clara; ya que la guía resultado de este trabajo se basará en buenas prácticas tanto de seguridad como de auditoría usadas actualmente, pero encaminadas evaluar la disponibilidad del servicios de infraestructura en la nube.

## **2. OBJETIVOS DEL PROYECTO**

### **2.1. OBJETIVO GENERAL**

Desarrollar una guía de auditoría para evaluar el aseguramiento de la disponibilidad de la información en un ambiente Cloud Computing IaaS, bajo la norma ISO 27001 de 2013.

### **2.2. OBJETIVOS ESPECÍFICOS**

- Caracterizar los dominios de la norma ISO 27001, para determinar los criterios a evaluar en términos de disponibilidad de la información.
- Estructurar una guía de auditoría basada en la norma ISO 19011 para ambiente Cloud Computing IaaS a partir de los dominios caracterizados.
- Validar la guía con un grupo de expertos en auditoría de sistemas.



### **3. ESTADO DEL ARTE**

#### **3.1. HISTORIA DEL CONCEPTO NUBE**

"El término "nube" se utiliza como una metáfora de Internet, basado en el dibujo de nubes utilizado en el pasado para representar a la red telefónica, y más tarde para representar a Internet en los diagramas de red de computadoras como una abstracción de la infraestructura subyacente que representa.

El cloud computing o computación en la nube es una evolución natural de la adopción generalizada de la virtualización, la arquitectura orientada a servicios y utilidad del cómputo. La idea básica es que los usuarios finales ya no necesitan tener conocimientos o el control sobre la infraestructura de tecnología "en la nube" que los apoya.

El concepto básico del cloud computing o computación en nube se le atribuye a John McCarthy - responsable de introducir el término "inteligencia artificial". En 1961, durante un discurso para celebrar el centenario del MIT, fue el primero en sugerir públicamente que la tecnología de tiempo compartido (Time-Sharing) de las computadoras podría conducir a un futuro donde el poder del cómputo e incluso aplicaciones específicas podría venderse como un servicio (tal como el agua o la electricidad). Esta idea de una computadora o utilidad de la información era muy popular en la década de 1960, incluso algunas empresas comenzaron a proporcionar recurso compartidos como oficina de servicios - donde se alquilaba tiempo y servicio de cómputo. El sistema de tiempo compartido proporcionaría un ambiente operacional completo, incluyendo editores de texto y entornos de desarrollo integrado para lenguajes de programación, paquetes de programas informáticos, almacenamiento de archivos, impresión masiva y de almacenamiento offline. A los usuarios se les cobraba un alquiler por el terminal, las horas de tiempo de conexión, tiempo del CPU y kilobytes mensuales de almacenamiento en disco. Sin embargo, esta popularidad se desvaneció a mediados de los 70s cuando quedó claro que el hardware, software y las tecnologías de comunicación simplemente no estaban preparados.

El concepto de una red de computadoras capaz de comunicar usuarios en distintas computadoras fue formulado por J.C.R. Licklider de Bolt, Beranek and Newman (BBN) en agosto de 1962, en una serie de notas que discutían la idea de una "Red Galáctica".

En 1996, Douglas Parkhill con su libro llamado "El desafío de la utilidad de la computadora" exploró a fondo muchas de las características actuales de la computación en nube (aprovisionamiento elástico a través de un servicio de utilidad), así como la comparación de la industria eléctrica y el uso de las formas públicas, privadas, comunitarias y gubernamentales. Pero otros investigadores

afirman que las raíces de la computación en nube nos llevan hasta la década de 1950 con las observaciones de Herb Grosch. Él decía que la potencia de una computadora es proporcional al cuadrado de su precio (Ley Grosch), sin embargo la ley de Moore se encargó de desmentir esto. Algunos académicos recientemente han rehabilitado la ley de Grosch, mirando la historia de la computación en la nube, afirman que "Grosch estaba equivocado sobre el modelo del costo de la computación en nube, no se equivocaba en su suposición de que las economías eficientes y adaptables podría alcanzar su objetivo si confían en centros de datos centralizados en lugar de confiar en el almacenamiento de unidades".

Las empresas de telecomunicaciones hasta la década de los 90s eran quienes ofrecían redes privadas virtuales (VPN) con una calidad de servicio semejante, pero a un costo mucho menor. Al ser capaces de equilibrar el tráfico pudieron hacer uso del ancho de banda total de la red con mayor eficacia. Incluso el símbolo de la nube se utiliza para indicar el punto de demarcación entre lo que es la responsabilidad del proveedor y lo que era la responsabilidad del usuario. Ahora la computación en nube extiende este límite para cubrir servidores, así como la infraestructura de red."<sup>7</sup>

Más adelante sobre los años 70, se adoptó el término computación grid.

### **3.2. COMPUTACIÓN GRID**

La computación en grid o malla fue el paradigma de la computación distribuida, en la cual todos los recursos de un número indefinido de computadoras son englobados como un único superordenador de forma transparente. Los orígenes de la computación grid se debe a la idea de compartición de recursos. La práctica conocida como "computación distribuida" nace aproximadamente en los años 50 y 60, pero solo hasta 1969 ya encontramos una definición por parte de Len Kleinrock "Grid es la infraestructura de hardware y software que proporciona un acceso serio, constante, penetrable y económico a capacidades computacionales de alta calidad", otra definición por Steve Tuecke "Grid computing es la compartición de recursos coordinados y de la solución de un problema en organizaciones virtuales dinámicas y multiinstitucionales"<sup>8</sup>

La computación grid es una tecnología innovadora que permite utilizar de forma coordinada todo tipo de recursos (entre ellos cómputo, almacenamiento y aplicaciones específicas) que no están sujetos a un control centralizado. En este sentido es una nueva forma de computación distribuida, en la cual los recursos

---

<sup>7</sup> BOXBYTE, El origen del Cómputo en la nube [en línea]. [citado en 22 de Agosto de 2014]. Disponible en internet: <<http://www.fayerwayer.com/2012/01/el-origen-de-el-computo-en-la-nube/>>

<sup>8</sup> COLOBRAN HUGUET Miguel, Administración de sistemas operativos en red: Administración de servidores. Barcelona: Editorial UOC, 2008. 37 p. ISBN: 978-84-9788-760-1

pueden ser heterogéneos (diferentes arquitecturas, supercomputadores y clusters) y se encuentran conectados mediante redes de área extensa (por ejemplo Internet)

La computación grid es el comienzo de la computación en la nube, que ha evolucionado con el concepto de entrega de aplicaciones empresariales y aprovisionamiento de servicios a través de la web.

### **3.3. GOOGLE FILE SYSTEM**

El sistema de archivado es otro avance hacia la computación en la nube. Google afirma que “ha diseñado e implementado el Sistema de archivos, un sistema de archivos distribuido escalable para grandes aplicaciones intensivas de datos distribuidas. Proporciona tolerancia a fallos durante la ejecución en hardware barato, y ofrece un alto rendimiento agregado a un gran número de clientes.

Aunque comparte muchos de los mismos objetivos que los sistemas de archivos distribuidos anteriores, este diseño ha sido impulsada por las observaciones de las cargas de trabajo de aplicación y el ambiente tecnológico, tanto actuales como previstos, que reflejan una marcada salida de algunos supuestos de sistemas de archivos anteriores. Esto ha llevado a reexaminar las opciones tradicionales y explorar radicalmente diferentes puntos de diseño.

El sistema de archivos se ha reunido con éxito necesidades de almacenamiento. Es ampliamente desplegado dentro de Google como la plataforma de almacenamiento para la generación y el tratamiento de los datos utilizados por nuestro servicio, así como los esfuerzos de investigación y desarrollo que requieren grandes conjuntos de datos. El grupo más grande hasta la fecha ofrece cientos de terabytes de almacenamiento a través de miles de discos en más de mil máquinas, y se accede a ella al mismo tiempo por cientos de clientes.

El sistema de archivos de Google, GFS (siglas de «Google File System»), es un sistema de almacenamiento basado en las necesidades de Google diseñado por Sanjay Ghemawat, Howard Gobioff y Shun-Tak Leung y presentado por primera vez en «19th ACM Symposium on Operating Systems Principles», Lake George, Nueva York, octubre de 2003.

Al no ser un sistema de archivos de uso generalista, GFS, ha sido diseñado teniendo en cuenta las siguiente premisas: que un componente falle es la norma no la excepción, los archivos son enormes (archivos de muchos GB son comunes), es muy común que un archivo cambie porque se le añaden datos pero es muy raro que se sobrescriban los datos existentes, el diseño de las aplicaciones y de la API del sistema de archivos proporciona un beneficio global.

Suposiciones:

- El sistema está construido para que el fallo de un componente no le afecte.
- El sistema almacena grandes archivos
- La mayoría del trabajo consiste en dos tipos de lecturas: grandes lecturas de datos y pequeñas lecturas aleatorias
- La carga de trabajo también consiste en añadir grandes secuencias de datos a archivos.
- El sistema debe ser diseñado para ofrecer concurrencia a múltiples clientes que quieran el mismo archivo.
- Tener un gran ancho de banda prolongadamente es más importante que una baja latencia."<sup>9</sup>

### **3.4. CLOUD COMPUTING EN LOS ÚLTIMOS AÑOS**

Los avances tecnológicos para ver más claramente la computación en la nube, se han dado en la última década, donde los modelos de cloud computing se han venido implementando, es uno de los casos el de Amazon, quien en "2006 también vio la introducción de Elastic Compute Cloud de Amazon (EC2) como un servicio web comercial que permitió a las empresas pequeñas y particulares alquilar equipos en los que pudieran ejecutar sus propias aplicaciones informáticas.

Este modelo de arquitectura fue immortalizado por George Gilder en su artículo de octubre 2006 en la revista Wired titulado "Las fábricas de información". Esto fue seguido por una colaboración de toda la industria en 2007 entre Google, IBM y una serie de universidades de los Estados Unidos. Luego vino Eucalyptus en 2008, como la primera plataforma de código abierto compatible con el API-AWS para el despliegue de Clouds privados, seguido por OpenNebula, el primer software de código abierto para la implementación de nubes privadas e híbridas. Microsoft entraría hasta el 2009 con el lanzamiento de Windows Azure. Luego en 2010 proliferaron servicios en distintas capas de servicio: Cliente, Aplicación, Plataforma, Infraestructura y Servidor. En 2011, Apple lanzó su servicio iCloud, un sistema de almacenamiento en la nube - para documentos, música, videos, fotografías, aplicaciones y calendarios - que prometía cambiar la forma en que usamos la computadora.

---

<sup>9</sup> GOOGLE, The Google File System [en línea]. [citado en 15 de Septiembre de 2014]. Disponible en internet: <<http://static.googleusercontent.com/media/research.google.com/es-419//archive/gfs-sosp2003.pdf> >

### **3.5. TIPOS DE NUBE**

Existen diversos tipos de nube dependiendo de las necesidades de cada empresa, el modelo de servicio ofrecido y la implementación de la misma, pero básicamente existen tres grandes grupos:

3.5.1. Nubes Públicas. Las nubes públicas se refieren al modelo estándar de computación en nube, donde los servicios que se ofrecen se encuentran en servidores externos al usuario, pudiendo tener acceso a las aplicaciones de forma gratuita o de pago.

3.5.2. Nubes Privadas. En las nubes privadas la plataforma se encuentra dentro de las instalaciones de la empresa y no suele ofrecer servicios a terceros. En general, una nube privada es una plataforma para la obtención solamente de hardware, es decir, máquinas, almacenamiento e infraestructura de red (IaaS), pero también se puede tener una nube privada que permita desplegar aplicaciones (PaaS) e incluso aplicaciones (SaaS).

Las nubes privadas son una buena opción para las compañías que necesitan alta protección de datos y ediciones a nivel de servicio. En las nubes privadas el cliente controla qué aplicaciones usa y cómo. La empresa es la propietaria de la infraestructura y puede decidir qué usuarios están autorizados a utilizarla.

3.5.3. Nubes Híbridas. Las nubes híbridas combinan recursos locales de una nube privada con la nube pública. La infraestructura privada se ve aumentada con los servicios de computación en nube de la infraestructura pública. Esto permite a una empresa mantener el control de sus principales aplicaciones y aprovechar la computación en nube pública solamente cuando resulte necesario."<sup>10</sup>

### **3.6. CLOUD COMPUTING**

"El Instituto Nacional de Normas y tecnología (NIST) de los EE.UU define el Cloud computing como "un modelo para habilitar un cómodo acceso en red omnipresente, a solicitud, a un conjunto compartido de recursos informáticos configurables (por ejemplo redes, servidores, recursos de almacenamiento o aplicaciones y servicios) que se pueden conformar y proveer rápidamente con un esfuerzo administrativo mínimo o una interacción mínima con el proveedor de servicios" , Así mismo NIST establece que el Cloud computing tiene tres modelos de servicio, dentro de los cuales están:

---

<sup>10</sup> CLOUD COMPUTING, Computación en nube [en línea]. [citado en 10 de Agosto de 2014]. Disponible en internet: <<http://www.computacionennube.org/13/tipos-de-nube/>>

3.6.1. Cloud Software as a Service (SaaS). “Con el concepto de Software como Servicio (SaaS, Software as a Service) se describe cualquier servicio cloud en el que los consumidores puedan acceder a aplicaciones de software a través de internet. Esas aplicaciones están alojadas "en la nube" y pueden utilizarse para una amplia variedad de tareas, tanto para particulares como para organizaciones. Google, Twitter, Facebook y Flickr son ejemplos de SaaS, en los cuales los usuarios pueden acceder a los servicios a través de cualquier dispositivo que pueda conectarse a internet. Los usuarios empresariales pueden utilizar aplicaciones para resolver necesidades muy diversas, desde la contabilidad y la facturación hasta el seguimiento de ventas, planificación, control de rendimiento y comunicaciones (por ejemplo, el correo web y la mensajería instantánea).

El modelo SaaS se conoce también a veces como "software a demanda", y la forma de utilizarlo se parece más a alquilar el software que a comprarlo. Con las aplicaciones tradicionales, el software se compra al principio como un paquete, y una vez adquirido se instala en el ordenador del usuario. La licencia del software puede también establecer limitaciones en cuanto al número de usuarios y/o dispositivos en los cuales puede instalarse. Por el contrario, los usuarios del Software como Servicio se suscriben al software, en lugar de comprarlo, generalmente por períodos mensuales. Las aplicaciones se compran y utilizan a través de internet, y los archivos se guardan en la nube, no en el ordenador del usuario.

Son varias las razones por las que el modelo SaaS resulta muy ventajoso tanto para empresas como para particulares:

- No tiene costes adicionales de hardware; la potencia de procesamiento necesaria para hacer funcionar las aplicaciones la proporciona el proveedor de la infraestructura cloud.
- No tiene costes de alta; las aplicaciones están listas para utilizarlas desde el momento en que el usuario se suscribe a ellas.
- Se paga sólo por lo que se utiliza; si un elemento de software sólo se va a necesitar durante un período limitado, se puede pagar únicamente durante ese período, y generalmente las suscripciones pueden cancelarse en cualquier momento.
- El uso del servicio es escalable; si un usuario decide que necesita más espacio de almacenamiento o contratar servicios adicionales, por ejemplo, puede acceder a esos servicios a demanda sin tener que instalar más hardware o software.
- Las actualizaciones son automáticas; cada vez que existe una actualización, queda disponible online de forma inmediata para los usuarios, a

menudo sin coste. No se necesitará ningún software nuevo, como ocurre con otros tipos de aplicaciones, y por lo general las actualizaciones serán desplegadas automáticamente por el proveedor del servicio cloud.

- Compatibilidad entre dispositivos; para acceder a las aplicaciones SaaS puede utilizarse cualquier dispositivo con conexión a internet, lo que las hace ideales para quienes utilizan muchos dispositivos diferentes, por ejemplo tablets y teléfonos con internet, así como para los que no siempre utilizan el mismo ordenador.
- Accesible desde cualquier lugar; en lugar de limitarse a instalaciones concretas en ordenadores específicos, la aplicación puede estar accesible para cualquiera que tenga un dispositivo capaz de conectarse a internet.
- Las aplicaciones pueden personalizarse y asociarse a la imagen de marca del proveedor; algunas aplicaciones de software pueden personalizarse, es decir, alterarse para adaptarlas a las necesidades y la imagen de marca de un determinado cliente.

El software ofimático es el mejor ejemplo posible de aplicación del modelo SaaS en la empresa. Todas las tareas relacionadas con la contabilidad, facturación, ventas y planificación pueden ejecutarse en la modalidad de Software como Servicio. A una empresa podría interesarle utilizar un determinado elemento de software que realice todas estas tareas, o bien varios diferentes para cada una de esas tareas. El cliente puede conseguir el software necesario suscribiéndose a él a través de internet, y a partir de ese momento acceder online a ese software desde cualquier ordenador de su oficina, con sólo introducir un nombre de usuario y una contraseña. Y si cambian sus necesidades, podrá cambiar fácilmente al software que mejor las resuelva. Cualquiera que necesite acceder a un determinado elemento de software puede darse de alta como usuario, tanto si se trata de sólo una o dos personas como si son todos los empleados de una gran organización con cientos de trabajadores.

Resumen del modelo:

- Con el modelo SaaS no hay costes de alta, tan habituales en otras aplicaciones
- El modelo SaaS es escalable, con actualizaciones disponibles a demanda
- El acceso al Software como Servicio es compatible con todo tipo de dispositivos capaces de conectarse a internet
- Las aplicaciones están accesibles desde cualquier lugar donde se disponga de una conexión a internet.

3.6.2. Cloud Platform as a Service (PaaS). El concepto de Plataforma como Servicio (PaaS, Plataform as a Service) es una categoría de servicios cloud que proporciona una plataforma y un entorno que permiten a los desarrolladores crear aplicaciones y servicios que funcionen a través de internet. Los servicios PaaS se

alojan en la nube, y los usuarios pueden acceder a ellos simplemente a través de su navegador web.

El modelo PaaS permite a los usuarios crear aplicaciones de software utilizando herramientas suministradas por el proveedor. Los servicios PaaS pueden consistir en funcionalidades preconfiguradas a las que los clientes puedan suscribirse, eligiendo las funciones que deseen incluir para resolver sus necesidades y descartando aquellas que no necesiten. Así, los paquetes pueden variar desde un sencillo entorno que se maneje con el ratón y no requiera ningún tipo de conocimiento o instalación especial por el lado del usuario, hasta el suministro de opciones de infraestructura para desarrollo avanzado.

La infraestructura y las aplicaciones se gestionan en nombre del cliente, y se ofrece también soporte técnico. Los servicios se actualizan constantemente, mejorando las funcionalidades existentes y añadiendo otras nuevas. Los proveedores de PaaS pueden colaborar con los desarrolladores desde la concepción de sus ideas originales hasta la creación de las aplicaciones, llegando incluso hasta las fases de pruebas e implantación. Y todo eso se consigue utilizando un solo mecanismo gestionado.

Al igual que en la mayoría de las propuestas de servicios cloud, los servicios PaaS suelen facturarse como una suscripción en la que el cliente acaba pagando al final sólo por lo que realmente utiliza. Además, puede beneficiarse de las economías de escala que aporta el hecho de estar compartiendo una misma infraestructura física subyacente entre muchos usuarios, lo que se traduce en una reducción de costes.

Estas son algunas de las funcionalidades que pueden incluirse dentro de una propuesta de PaaS:

- Sistema operativo
- Entorno de scripting de servidor
- Sistema de gestión de base de datos
- Software de servidor
- Soporte técnico
- Almacenamiento
- Acceso a la red
- Herramientas de diseño y desarrollo
- Hosting.

El modelo PaaS aporta ventajas tanto a los desarrolladores de software como a los programadores de webs y a las empresas. Tanto si se trata de crear una aplicación que tengan previsto ofrecer a través de internet como de un software para vender en las tiendas, una solución PaaS proporciona grandes ventajas a un



desarrollador de software. Por ejemplo, los desarrolladores para web pueden utilizar entornos PaaS diferentes en cada una de las fases del proceso de creación de sus webs, desde el desarrollo hasta las pruebas y su alojamiento final. Y también las empresas que desarrollan internamente su propio software pueden sacar partido al modelo de Plataforma como Servicio, por ejemplo para crear entornos de pruebas y de desarrollo completamente aislados entre sí.

Estas son algunas de las ventajas que aporta el modelo PaaS a los desarrolladores de aplicaciones:

- *No necesitan invertir en infraestructura física*; poder "alquilar" una infraestructura virtual les supone ventajas tanto económicas como prácticas. Les evita tener que comprar hardware por su cuenta y dedicar sus conocimientos a administrarlo, lo cual les deja más tiempo libre para concentrarse en el desarrollo de las aplicaciones. Además, los clientes sólo necesitarán alquilar los recursos que necesiten, en lugar de invertir en capacidad fija que vaya a permanecer sin utilizarse y por tanto suponer malgastar recursos.
- Hace posible que incluso usuarios "no expertos" puedan realizar desarrollos; con algunas propuestas de PaaS, cualquiera puede desarrollar una aplicación. Sólo tiene que seguir los pasos necesarios a través de una sencilla interfaz web. Un excelente ejemplo de este tipo de aplicaciones son las instalaciones de software para la gestión de blogs como WordPress.
- *Flexibilidad*; los clientes pueden disfrutar de un control total sobre las herramientas que se instalen en sus plataformas, y crear una plataforma perfectamente adaptada a sus necesidades concretas. Sólo tienen que ir seleccionando aquellas funcionalidades que consideren necesarias.
- *Adaptabilidad*; las funcionalidades pueden modificarse si las circunstancias así lo aconsejan.
- Permite la colaboración entre equipos situados en varios lugares distintos; como lo único que se necesita es una conexión a internet y un navegador web, los desarrolladores pueden estar dispersos por varios lugares distintos y aun así colaborar juntos en el desarrollo de la misma aplicación.
- Seguridad; se ofrecen diversos mecanismos de seguridad, que incluyen la protección de los datos y la realización y recuperación de copias de seguridad.
- En resumen, una propuesta de PaaS proporciona un entorno de trabajo para el desarrollo de aplicaciones. En otras palabras, ofrece la arquitectura así como la infraestructura general necesaria para permitir el desarrollo de aplicaciones, lo que incluye recursos de red, almacenamiento de datos, y servicios de administración de software y soporte técnico. Por tanto, se trata de un concepto ideal para el desarrollo de nuevas aplicaciones orientadas tanto a la web como a dispositivos móviles y PCs.<sup>11</sup>

---

<sup>11</sup> NIST, The NIST definition of Cloud computing, Special Publication 800-145 [en línea]. [citado 12 de agosto de 2014]. Disponible en internet: <<http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>>

3.6.3. Cloud Infrastructure as a Service (IaaS). “El concepto de Infraestructura como Servicio (IaaS, Infrastructure as a Service) es uno de los tres modelos fundamentales en el campo del cloud computing, junto con el de Plataforma como Servicio (PaaS, Platform as a Service) y el de Software como Servicio (SaaS, Software as a Service). Al igual que todos los servicios cloud, IaaS proporciona acceso a recursos informáticos situados en un entorno virtualizado, la "nube" (cloud), a través de una conexión pública, que suele ser internet. En el caso de IaaS, los recursos informáticos ofrecidos consisten, en particular, en hardware virtualizado, o, en otras palabras, infraestructura de procesamiento. La definición de IaaS abarca aspectos como el espacio en servidores virtuales, conexiones de red, ancho de banda, direcciones IP y balanceadores de carga. Físicamente, el repertorio de recursos de hardware disponibles procede de multitud de servidores y redes, generalmente distribuidos entre numerosos centros de datos, de cuyo mantenimiento se encarga el proveedor del servicio cloud. El cliente, por su parte, obtiene acceso a los componentes virtualizados para construir con ellos su propia plataforma informática.

El modelo IaaS coincide con las otras dos modalidades de hosting cloud en que puede ser utilizado por los clientes empresariales para crear soluciones informáticas económicas y fáciles de ampliar, en las cuales toda la complejidad y el coste asociados a la administración del hardware subyacente se externaliza al proveedor del servicio cloud. Si la escala o el volumen de actividad del negocio del cliente fluctúan, o si la empresa tiene previsto crecer, puede recurrir al recurso cloud en el momento y de la manera en que lo necesite, en lugar de tener que adquirir, instalar e integrar hardware por su cuenta.

Estos son varios ejemplos representativos de aplicaciones concretas del modelo IaaS para una gran empresa:

- *Infraestructura corporativa*; las redes internas de la empresa, como las Clouds privadas y las redes locales virtuales, que utilizan recursos de red y de servidores agrupados en un repertorio común, donde la empresa puede almacenar sus datos y ejecutar las aplicaciones que necesite para su funcionamiento diario. Las empresas en crecimiento pueden ampliar su infraestructura a medida que aumente su volumen de actividad, mientras que las clouds privadas (accesibles sólo para la propia empresa) permiten proteger el almacenamiento y transferencia de los datos delicados que algunas empresas necesitan manejar.
- *Hosting cloud*; alojamiento de las webs en servidores virtuales que funcionan sobre recursos comunes materializados físicamente en servidores físicos subyacentes. Una web alojada en una plataforma cloud, por ejemplo, puede beneficiarse de la redundancia que aporta la gigantesca escala de la red de servidores físicos y su escalabilidad en función de la demanda para afrontar cualquier punta inesperada de tráfico en su web.

- *Virtual Data Centers (VDC)*; una red virtualizada de servidores virtuales interconectados que puede utilizarse para ofrecer funcionalidades avanzadas alojadas en un entorno cloud, para implementar la infraestructura informática de la empresa, o para integrar todas esas operaciones dentro de una implementación cloud pública o privada.
- Estas son las ventajas características de una implementación basada en el modelo de Infraestructura como Servicio:
- *Escalabilidad*; los recursos están disponibles de la manera y en el momento en que el cliente los necesita, por lo que desaparecen los tiempos de espera a la hora de ampliar la capacidad, y no se desaprovecha la capacidad que no se esté utilizando.
- Sin necesidad de invertir en hardware; el hardware físico subyacente sobre el que funciona el servicio IaaS es configurado y mantenido por el proveedor del servicio cloud, lo que evita tener que dedicar tiempo y dinero a realizar esa instalación en el lado del cliente
- Modelo de tarificación similar al de los suministros públicos como la luz o el gas; el servicio está accesible a demanda, y el cliente sólo paga por los recursos que realmente utiliza
- Independencia de la localización; por lo general, se puede acceder al servicio desde cualquier lugar, siempre y cuando se disponga de una conexión a internet y el protocolo de seguridad del servicio cloud lo permita
- Seguridad física en los centros de datos; los servicios disponibles a través de una infraestructura cloud pública, o en clouds privadas alojadas externamente en las instalaciones del proveedor del servicio cloud, se benefician de la seguridad física de que disfrutaban los servidores alojados dentro de un centro de datos
- No hay puntos únicos de fallo; si falla un servidor o un conmutador, el servicio global no se verá afectado, gracias a la gran cantidad restante de recursos de hardware y configuraciones redundantes. En muchos servicios, incluso la caída de un centro de datos entero, y no digamos de un solo servidor, no afecta en absoluto al funcionamiento del servicio IaaS."<sup>12</sup>

FIGURA 3. MODELO CLOUD COMPUTING

---

<sup>12</sup> INTERNAUTE, Cloud Computing, [en línea]. [citado 22 de agosto de 2014]. Disponible en internet: <<http://www.interoute.es/>>



Fuente: NIST Visual Model of Cloud Computing Definition<sup>13</sup>

La figura ilustra de manera clara como se articulan los modelos y servicios mencionados y expone las principales características que tiene el modelo Cloud Computing.

### 3.7. CASOS DE ÉXITO DE COMPUTACIÓN EN LA NUBE

Algunos de los casos de éxito de computación en la nube son los siguientes:

3.7.1. Avanzo. "Avanzo por su experiencia en el modelo de Cloud Computing fue el socio de Proexport en un proyecto denominado "CRM para PYMES Exportadoras", en el que la pequeña y mediana empresa es subsidiada por Proexport con el 50% para la implementación de un proyecto de CRM. La tecnología seleccionada fue Salesforce.com por su facilidad de uso y rapidez de implementación. El proyecto en su totalidad tomó dos años y se implementó con resultados muy positivos en aproximadamente, 135 empresas PYMES en toda Colombia, de diversas industrias: flores, construcción, metalmecánica, alimentos, confecciones, servicios, tecnología y salud, entre otras. Estas empresas nunca se hubieran acercado a tecnología de punta como es Salesforce.com, ni a una teoría organizacional como es el CRM (que es la administración de la relación con el cliente), si no hubieran existido dos elementos: Primero que no existiera una complejidad asociada al proyecto y eso lo garantiza Cloud Computing. Lo otro, que existió el subsidio por parte del Gobierno y esto venció la resistencia y el miedo a ese riesgo de invertir o no en tecnología. Esto tomando en cuenta que las PYMES consideran la tecnología como un gasto no como una inversión. El

<sup>13</sup> Cloud Security Alliance, Security Guidance for critical areas of focus Cloud computing V2.1 [en línea]. EE.UU: NIST [citado en 12 de Agosto de 2014]. Disponible en internet: <https://cloudsecurityalliance.org/guidance/csaguide.pdf>

objetivo del proyecto era cambiar esa mentalidad y ha sido muy exitoso. Incluso en CINTEL fue postulado como una de los proyectos de tecnología del año.

3.7.2. Novartis. Esta fue una implementación en 20 países; asociada a mejorar la fidelización y el conocimiento del paciente que es cliente de Novartis. El proyecto cuenta con elementos de complejidad adicionales, a los específicamente tecnológicos, debido a la multiplicidad de países y por lo tanto son 20 regulaciones diferentes con procesos comerciales también distintos los cuales Avanzo logró que se pusieran en marcha todos sobre una sola tecnología a través de un modelo flexible y escalable, que entró a funcionar muy rápidamente con éxito.

3.7.3. Avantel - Gmail transforma las comunicaciones. La empresa de telecomunicaciones móviles Avantel adoptó la plataforma de Google Apps para solucionar problemas y limitaciones con sus sistemas de correo y mensajería, afectaban la productividad de sus empleados. El fácil acceso a las aplicaciones, la mejor relación costo/beneficio, la alta disponibilidad y el respaldo de Google fueron las razones que Avantel tuvo para optar por la plataforma en la nube de Google.

La empresa realizó un proyecto piloto con 50 cuentas empresariales, que le permitió probar las características funcionales del producto. Posteriormente, implementó nuevas cuentas de manera gradual en todas las dependencias de las oficinas principales en Bogotá, para finalmente habilitar las cuentas en las diferentes sucursales a lo largo del país. Dada la magnitud del proyecto, Avantel se apoyó en Eforcers, firma experta y certificada en Google Apps, para que instalara la plataforma, migrará los datos de la antigua y capacitara a los empleados en el uso de las herramientas

En cuanto al correo, los empleados de Avantel venían trabajando con sistemas de almacenamiento de correos con una cuota limitada, que se multiplicaron por 50 con Google Apps Premier Edition y su servicio Gmail (25 GB). Con este cambio, 497 empleados drásticamente sus comunicaciones electrónicas al no tener limitaciones en sus buzones. Además, contar con diferentes alternativas de acceso al correo –cualquier computador con acceso a Internet, así como dispositivos móviles– representó más beneficios.

El gran impacto de Google Apps Premier Edition, especialmente con Gmail, no sólo ha transformado las comunicaciones de los empleados, sino también su productividad y movilidad. Además, ha generado nuevas ideas comerciales por parte de la compañía, como la de llevar los beneficios de Gmail a las unidades móviles de sus clientes, lo cual le permitiría ofrecer un valor agregado a sus clientes y una ventaja competitiva a Avantel.

SSP: reducción del 98% en requerimientos de soporte. La Superintendencia de Servicios Públicos Domiciliarios es una de las entidades del Estado colombiano

pioneras en adoptar Google Apps Premier. La SSP tenía varios objetivos para implementar esta solución: la flexibilidad que podría brindar a los usuarios para comunicarse –por correo, mensajería instantánea y videoconferencia– y para colaborar en documentos compartidos en línea, y los bajos costos mensuales, que permitirían drásticamente su presupuesto en TI, al reducir el número de servidores y otros equipos, así como los costos de administración y soporte técnico.

Hoy, más de 850 usuarios de la SSP utilizan Google Apps Premier como su plataforma de uso permanente, y además de lograr los objetivos de flexibilidad y reducción de costos, obtuvo un importante beneficio adicional: la reducción de los requerimientos de soporte técnico de un 98%, que le ha permitido al personal de TI concentrarse en labores más importantes que la solución de problemas.

3.7.4. Fedepalma del correo a la colaboración. Para resolver sus crecientes necesidades en comunicación y gestión de información, la Federación Nacional de Cultivadores de Palma de Aceite, decidió adoptar Google Apps Premier Edition en sus sedes de Bogotá, Villavicencio (Meta) y Cumaral (Casanare), además de las sedes del Centro de Investigación en Palma de Aceite, Cenipalma, en Bogotá, Villavicencio, Tumaco (Nariño), Barrancabermeja (Santander) y Fundación (Magdalena).

La implementación de Google Apps Premier Edition, realizada por la firma Eforcers, facilitó las comunicaciones en las seis sedes del gremio palmicultor en el país, que a su vez se reflejó en un incremento en su productividad. Fedepalma encontró en la plataforma de Google y en particular en Gmail la solución para sus necesidades de comunicación robusta, confiable y segura, y con una capacidad de almacenamiento que con las plataformas tradicionales sería difícil de imaginar.

Pero más allá de los beneficios de Gmail para los 240 usuarios de Fedepalma y Cenipalma, éstos también se comunican por mensajería y videoconferencia a través de Google Talk, agendan tareas y reuniones con Calendar y han empezado a editar documentos compartidos con Google Docs, lo que les ha brindado nuevas opciones de colaboración."<sup>14</sup>

### **3.8. SEGURIDAD DE LA INFORMACIÓN**

Existen muchas definiciones del término seguridad. Simplificando, y en general, podemos definir la seguridad como: Característica que indica que un sistema está libre de todo peligro, daño o riesgo.

---

<sup>14</sup> ARIEL Alonso, Cloud Computing [en línea]. [citado el 25 de Agosto de 2014]. Disponible en internet: < <http://cloudcomputingug.wordpress.com/casos-de-exito/>>

Cuando se habla de seguridad de la información se indica que dicha información tiene una relevancia especial en un contexto determinado y que, por tanto, hay que proteger.

La Seguridad de la Información se puede definir como conjunto de medidas técnicas, organizativas y legales que permiten a la organización asegurar la confidencialidad, integridad y disponibilidad de su sistema de información.

Hasta la aparición y difusión del uso de los sistemas informáticos, toda la información de interés de una organización se guardaba en papel y se almacenaba en grandes cantidades de abultados archivadores. Datos de los clientes o proveedores de la organización, o de los empleados quedaban registrados en papel, con todos los problemas que luego acarrea su almacenaje, transporte, acceso y procesado.

Los sistemas informáticos permiten la digitalización de todo este volumen de información reduciendo el espacio ocupado, pero, sobre todo, facilitando su análisis y procesado. Se gana en 'espacio', acceso, rapidez en el procesado de dicha información y mejoras en la presentación de dicha información.

Pero aparecen otros problemas ligados a esas facilidades. Si es más fácil transportar la información también hay más posibilidades de que desaparezca 'por el camino'. Si es más fácil acceder a ella también es más fácil modificar su contenido, etc.

Desde la aparición de los grandes sistemas aislados hasta nuestros días, en los que el trabajo en red es lo habitual, los problemas derivados de la seguridad de la información han ido también cambiando, evolucionando, pero están ahí y las soluciones han tenido que ir adaptándose a los nuevos requerimientos técnicos. Aumenta la sofisticación en el ataque y ello aumenta la complejidad de la solución, pero la esencia es la misma.

Existen también diferentes definiciones del término Seguridad Informática. De ellas nos quedamos con la definición ofrecida por el estándar para la seguridad de la información ISO/IEC 27001, que fue aprobado y publicado en octubre de 2005 por la International Organization for Standardization (ISO) y por la comisión International Electrotechnical Commission (IEC).

“La seguridad informática consiste en la implantación de un conjunto de medidas técnicas destinadas a preservar la confidencialidad, la integridad y la disponibilidad de la información, pudiendo, además, abarcar otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio.”<sup>15</sup>

---

<sup>15</sup> OBSERVATORIO TECNOLÓGICO, Seguridad informática [en línea]. España: Elvira Mifsud [citado 12 Octubre de 2014]. Disponible en internet:

En seguridad de la información se menciona el término de Fiabilidad, que no es otra cosa que la probabilidad de que un sistema se comporte tal cual como se espera de él, en estos términos se deben considerar tres aspectos importantes:

- **Confidencialidad:** En general el término 'confidencial' hace referencia a (Que se hace o se dice en confianza o con seguridad recíproca entre dos o más personas.)

En términos de seguridad de la información, la confidencialidad hace referencia a la necesidad de ocultar o mantener secreto sobre determinada información o recursos.

El objetivo de la confidencialidad es, entonces, prevenir la divulgación no autorizada de la información.

En general, cualquier empresa pública o privada y de cualquier ámbito de actuación requiere que cierta información no sea accedida por diferentes motivos. Uno de los ejemplos más típicos es el del ejército de un país. Además, es sabido que los logros más importantes en materia de seguridad siempre van ligados a temas estratégicos militares.

Por otra parte, determinadas empresas a menudo desarrollan diseños que deben proteger de sus competidores. La sostenibilidad de la empresa así como su posicionamiento en el mercado puede depender de forma directa de la implementación de estos diseños y, por ese motivo, deben protegerlos mediante mecanismos de control de acceso que aseguren la confidencialidad de esas informaciones.

Un ejemplo típico de mecanismo que garantice la confidencialidad es la Criptografía, cuyo objetivo es cifrar o encriptar los datos para que resulten incomprensibles a aquellos usuarios que no disponen de los permisos suficientes.

Pero, incluso en esta circunstancia, existe un dato sensible que hay que proteger y es la clave de encriptación. Esta clave es necesaria para que el usuario adecuado pueda descifrar la información recibida y en función del tipo de mecanismo de encriptación utilizado, la clave puede/debe viajar por la red, pudiendo ser capturada mediante herramientas diseñadas para ello. Si se produce esta situación, la confidencialidad de la operación realizada (sea bancaria, administrativa o de cualquier tipo) queda comprometida.



- **Integridad:** En general, el término 'integridad' hace referencia a una cualidad de 'íntegro' e indica "Que no carece de ninguna de sus partes." y relativo a personas "Recta, proba, intachable."

En términos de seguridad de la información, la integridad hace referencia a la fidelidad de la información o recursos, y normalmente se expresa en lo referente a prevenir el cambio impropio o desautorizado.

El objetivo de la integridad es, entonces, prevenir modificaciones no autorizadas de la información.

La integridad hace referencia a:

- La integridad de los datos (el volumen de la información)
- La integridad del origen (la fuente de los datos, llamada autenticación)
- Es importante hacer hincapié en la integridad del origen, ya que puede afectar a su exactitud, credibilidad y confianza que las personas ponen en la información.

A menudo ocurre que al hablar de integridad de la información no se da en estos dos aspectos. Por ejemplo, cuando un periódico difunde una información cuya fuente no es correcta, podemos decir que se mantiene la integridad de la información ya que se difunde por medio impreso, pero sin embargo, al ser la fuente de esa información errónea no se está manteniendo la integridad del origen, ya que la fuente no es correcta.

- **Disponibilidad:** En general, el término 'disponibilidad' hace referencia a una cualidad de 'disponible' y dicho de una cosa "Que se puede disponer libremente de ella o que está lista para usarse o utilizarse."

En términos de seguridad de la información, la disponibilidad hace referencia a que la información del sistema debe permanecer accesible a elementos autorizados.

El objetivo de la disponibilidad es, entonces, prevenir interrupciones no autorizadas/controladas de los recursos informáticos.

En términos de seguridad informática "un sistema está disponible cuando su diseño e implementación permite deliberadamente negar el acceso a datos o servicios determinados". Es decir, un sistema es disponible si permite no estar disponible. "Y un sistema 'no disponible' es tan malo como no tener sistema. No sirve."<sup>16</sup>

---

<sup>16</sup> OBSERVATORIO TECNOLÓGICO, Seguridad informática [en línea]. España: Elvira Mifsud [citado 12 Octubre de 2014]. Disponible en internet:

En conclusión la seguridad consiste en mantener el equilibrio adecuado entre estos tres factores. No tiene sentido conseguir la confidencialidad para un dato si no está disponible o si ha sido modificado. Dependiendo del entorno de trabajo y sus necesidades se puede dar prioridad a un aspecto de la seguridad o a otro. En ambientes militares suele ser siempre prioritaria la confidencialidad de la información frente a la disponibilidad. Aunque alguien pueda acceder a ella o incluso pueda eliminarla no podrá conocer su contenido y reponer dicha información será tan sencillo como recuperar una copia de seguridad.

En otros ambientes es prioritaria siempre la integridad de la información frente a la confidencialidad o disponibilidad. Se considera menos dañino que un usuario pueda leer un dato de otro usuario a que pueda modificarlo.

En un modelo de computación en la nube IaaS, la disponibilidad del servicio es esencial y prioritario, ya que provee todos los servicios de infraestructura a una o varias organizaciones. La interrupción del mismo podría ocasionar implicaciones legales y económicas tanto al proveedor del servicio como al dueño de la información. Es pensado en esto que se crean los acuerdos de nivel de servicio.

### **3.9. ACUERDOS DE NIVEL DE SERVICIO**

Los acuerdos de nivel de servicio son un punto clave al evaluar o medir la disponibilidad de un servicio en la nube, estos SLN's permiten establecer el referente que proporciona el servicio, las responsabilidades y los términos.

Esta es una revisión de la sección acuerdos de nivel de servicio de "Cloud Computing Use Cases Whitepaper" Versión 4.0 — publicada por el Cloud Computing Use Cases Discussion Group — para destacar los inconvenientes relacionados con los acuerdos de nivel de servicio que los arquitectos y desarrolladores deberían tener en cuenta cuando se trasladan a la nube.

#### **3.9.1. Qué es un ANS.**

- La lista de servicios que proporciona el proveedor y una definición completa de cada servicio.
- Las métricas para determinar si el proveedor está suministrando los servicios tal como lo prometió y un mecanismo de auditoría para monitorear el servicio.
- Las responsabilidades del proveedor y el consumidor y los recursos disponibles para ambos si los términos del ANS no se cumplen.

Una descripción de cómo el ANS se modificará con el correr del tiempo. Los dos tipos de ANSs, acuerdos listos para la venta y acuerdos negociados personalizados. Ellos señalan que los clientes con necesidades de datos críticos no estarán satisfechos con acuerdos listos para la venta, de modo de un primer paso antes de ir a la nube es determinar cuán críticos son sus datos y aplicaciones.

Las nubes públicas a menudo ofrecen un ANS no negociable que puede no ser aceptable para quienes poseen aplicaciones o datos de misión crítica.

3.9.2. Qué es un ONS. Un ANS contiene objetivos de nivel de servicio u ONS (services level objectives o SLOs en inglés) que definen las condiciones objetivamente medibles para el servicio; algunos ejemplos son los parámetros de rendimiento, y la frecuencia y la sincronización de la corriente de datos, los porcentajes de disponibilidad para VMs y otros recursos e instancias, o las valoraciones de las urgencias para clasificar la importancia de los diferentes ONSs (como "la disponibilidad es más importante que el tiempo de respuesta").

Lo que se espera de los ONSs debería variar según las aplicaciones y los datos a los que tienen acceso las aplicaciones están hospedados en la misma nube o en nubes diferentes.

3.9.3. Monitoreo y medición. La administración del nivel de servicio, basada en ONSs, es la forma de reunir y administrar la información de performance en la nube. Este es el modo en el cual se la emplea:

- El proveedor de la nube utiliza la administración de nivel de servicio para tomar decisiones relacionadas con la infraestructura; por ejemplo, si el rendimiento no siempre cumple con los requisitos del cliente, el proveedor puede reubicar el ancho de banda o agregar más hardware. O decidir hacer feliz a un cliente a expensas de otro. Para los proveedores, SLM ha sido diseñado para ayudar a tomar las mejores decisiones en base a los objetivos empresariales y las realidades técnicas.
- El consumidor de la nube utiliza SLM para decidir cómo desea usar los servicios de la nube; por ejemplo, si agregar o no más máquinas virtuales y a qué precio se determinará que esa opción es demasiado cara como para justificar los beneficios que acarrea. Para los clientes, SLM los ayuda a tomar decisiones en el modo en el cual utilizan la nube. Y a veces sobre cómo automatizar dichas decisiones.

3.9.4. Factores deberían considerarse en los términos del SLA. Lista de 10 factores que se deben tener en cuenta al definir los términos de un ANS:

- **Los objetivos de nivel empresarial:** una organización debe definir por qué utilizará los servicios de la nube antes de definir exactamente qué servicios utilizará. Esta parte está más relacionada con cuestiones del área de la política organizativa que del área técnica: algunos grupos pueden obtener recortes de presupuesto o perder el control de su infraestructura.
- **Las responsabilidades de ambas partes:** es importante definir el balance de las responsabilidades entre el proveedor y el consumidor. Por ejemplo, el proveedor será responsable por los aspectos de Software-as-a-Service (Software como Servicio), pero el consumidor puede generalmente ser responsable por su VM, la cual contiene software registrado y trabaja con datos sensibles.
- **Continuidad empresarial/recuperación de desastres:** el consumidor asegura que el proveedor tiene una protección contra desastres adecuada. Dos ejemplos nos vienen a la mente: el almacenamiento de datos valiosos en la nube como backups y cloud bursting o rebalse de nubes (se intercambian cuando los centros de datos internos no pueden encargarse del procesamiento de las cargas).
- **Redundancia:** evalúe cuán redundantes son los sistemas de su proveedor.
- **Mantenimiento:** uno de los aspectos más agradables del uso de la nube es que el proveedor administra el mantenimiento. Pero cuando los proveedores realizan las tareas de mantenimiento, los consumidores deberían saber:
  - ¿Los servicios no estarán disponibles durante este tiempo?
  - ¿Estarán disponibles los servicios pero el rendimiento será mucho menor?
  - ¿El consumidor tendrá la oportunidad de comparar sus aplicaciones con el servicio actualizado?
- **Ubicación de los datos:** existen regulaciones con ciertos tipos de datos que sólo pueden almacenarse en ubicaciones físicas determinadas. Los proveedores pueden responder a esos requisitos con la garantía de que los datos del consumidor serán almacenados solamente en ciertas ubicaciones y con la habilidad de auditar la situación.
- **Embargo de datos:** si por cumplimiento de la ley se embarga el equipo de un proveedor para capturar los datos y las aplicaciones que pertenecen a un consumidor en particular, dicho embargo probablemente afecte a otros consumidores que utilizan el mismo proveedor. Evalúe la posibilidad de que una tercera parte proporcione backup adicional.
- **Error del proveedor:** realice planes de contingencia que tengan en cuenta el estado financiero del proveedor.

- **Jurisdicción:** de nuevo, comprenda las leyes locales que se aplican a su proveedor, al igual que comprende las leyes que se aplican a usted.
- **Agentes de bolsa y revendedores:** si su proveedor es un agente de bolsa o un revendedor de servicios nube, debe comprender las políticas de su proveedor y al actual proveedor.

3.9.5. Requisitos del ANS. Lista de 14 responsabilidades a tener en cuenta al evaluar un ANS:

- **Seguridad:** un consumidor debe comprender sus requisitos de seguridad y qué controles y patrones de federación son necesarios para cubrir dichos requisitos. Un proveedor debe comprender lo que debe ofrecer al consumidor para permitir los controles y los patrones de federación correspondientes.
- **Encriptamiento de datos:** los datos deben ser encriptados mientras que se encuentren en movimiento y mientras se encuentran en reposo. Los detalles de los algoritmos de encriptamiento y las políticas de control de acceso deberían especificarse.
- **Privacidad:** las principales preocupaciones relacionadas con la privacidad están relacionadas con los requisitos como el encriptamiento, la conservación y la eliminación de datos. Un ANS debería aclarar cómo el proveedor nube aísla los datos y las aplicaciones en un entorno multi-tenant.
- **Conservación y eliminación de datos:** ¿cómo comprueba su proveedor que cumple con las leyes para la retención y las políticas de eliminación de datos?
- **Borrado y destrucción de hardware:** (Conservación y eliminación de datos)
- **Cumplimiento regulatorio:** Si las regulaciones deben implementarse según el tipo de datos, el proveedor nube debe ser capaz de probar que cumple con las mismas.
- **Transparencia:** en el caso de datos y aplicaciones críticas, los proveedores deben notificar por adelantado a los consumidores cuando no se respetan los términos del ANS. Esto incluye las cuestiones de infraestructura, como las interrupciones y los problemas de performance, además de los incidentes relativos a la seguridad.
- **Certificación:** el proveedor debería responsabilizarse por el suministro de la certificación necesaria y por mantenerse al día.

- **Definiciones de performance:** ¿Qué significa uptime? ¿Todos los servidores en todos los continentes están disponibles? ¿O sólo uno está disponible? Vale la pena aclarar estas definiciones. (Los autores de este paper sugieren estandarizar la terminología de la performance para que esto resulte más sencillo.)
- **Monitoreo:** por cuestiones de posibles incumplimientos, quizá desee determinar una organización de terceros que sea neutral para monitorear la performance del proveedor.
- **Auditabilidad:** dado que el consumidor es responsable por los incumplimientos que ocurrieran y provocaran pérdida de datos o de disponibilidad, es vital que el consumidor pueda auditar los sistemas y procedimientos del proveedor. El SLA debería dejar claro cómo y cuándo tendrán lugar dichas auditorías. Estas pueden ser perjudiciales y costosas para el proveedor.
- **Métricas:** estas son algunas de las cosas tangibles que pueden monitorearse cuando suceden y realizar la auditoría después. Las métricas de un ANS deben definirse objetivamente y con claridad. A continuación encontrará una lista de las métricas comunes.
- **Suministro de un ANS legible por máquina:** esto puede permitir una selección dinámica y automatizada de un agente nube. En otras palabras, si su ANS requiere que el agente utilice el proveedor más económico posible para algunas tareas pero el más seguro para otras, este tipo de automatización lo hace posible. (Este tipo de servicio no se encuentra fácilmente disponible aún, pero es algo para tener en cuenta al contribuir con el análisis de estandarización del ANS de la nube.
- **Interacción humana:** el autoservicio a pedido es una de las características principales de la computación en nube, pero su SLA debería tener en cuenta que cuando usted necesita un ser humano, podrá contar con uno.

Algunas de las métricas de performance comunes (Métricas) son las siguientes:

- Rendimiento: velocidad de respuesta del sistema.
- Confiabilidad: disponibilidad del sistema.
- Balanceo de la carga: cuando contribuye la elasticidad.
- Durabilidad: probabilidad de perder los datos.
- Elasticidad: cuánto puede crecer un recurso.
- Linealidad: performance del sistema a medida que aumenta la carga.
- Agilidad: rapidez de repuesta del proveedor ante las variaciones de carga.
- Automatización: porcentaje de solicitudes administradas sin intervención humana.

- Tiempos de respuesta del servicio al cliente.

Algunas normas fundamentales sobre la responsabilidad. Los autores proporcionan un tratado conciso sobre una definición del trabajo de la responsabilidad relacionada con la performance en la nube. Este dice más o menos lo siguiente:

- **La regla de los nueves.** Una métrica común relacionada con la responsabilidad es la cantidad de nueves que ofrece un proveedor (por ejemplo, si el servicio está disponible el 99.99999 % del tiempo, cinco nueves, entonces las interrupciones totales del sistema son de unos 5 minutos cada 12 meses). El problema es, ¿Qué es una interrupción? (Puede resultar una situación muy negativa si el proveedor llega a decidir lo que es una interrupción.)
- **Las capas de las nubes.** Muchos ofrecimientos nube están contruidos sobre otros ofrecimientos nube — esto es muy bueno para la flexibilidad y la potencia pero cada proveedor adicional hace que el sistema sea menos confiable. (Como si se estimara cada uno a cinco nueves, entonces el sistema en su conjunto es menor a cinco nueves.)
- **Distancia entre su aplicación y sus datos.** Nuevamente, a medida que la cantidad de proveedores aumenta, otros factores que pueden afectar la responsabilidad se afirman. No sólo se encuentra usted afectado cuando uno de los sistemas cae, también se ve afectado cuando cae la red entre ellos.<sup>17</sup>

### 3.10. CLASIFICACIÓN TIER EN EL DATACENTER.<sup>18</sup>

El TIER de un Datacenter es una clasificación ideada por el Uptime Institute que se plasmó en el estándar ANSI/TIA-942 y que básicamente establece (a día de hoy) 4 categorías, en función del nivel de redundancia de los componentes que soportan el Datacenter.

---

<sup>17</sup> IBM, Cloud Computing Use Cases Whitepaper [en línea]. IBM [citado en 20 de septiembre de 2014]. Disponible en internet: <<http://www.ibm.com/developerworks/ssa/cloud/library/cl-rev2sla.html>>

<sup>18</sup> TIA TR-42 Telecommunications Cabling Systems engineering committee recently released a second addendum to the TIA-942 Data Centers standard [en línea]. [citado en 18 de septiembre de 2014]. Disponible e internet < <http://www.tiaonline.org/news-media/news-articles/tia-942-data-center-cabling-standard-amended> >

FIGURA 4. NIVELES TIER EN DATACENTER



Fuente: Tycsa – centro de datos<sup>19</sup>

La figura ilustra las características básicas de cada uno de los niveles del TIER

3.10.1. **TIER I:** Centro de datos Básico. Es una instalación que no tiene redundadas sus componentes vitales (climatización, suministro eléctrico) y que por tanto perderá su capacidad de operación ante el fallo de cualquiera de ellas.

Puede o no puede tener suelos elevados, generadores auxiliares o UPS.

Del mismo modo, las operaciones de mantenimiento derivarán en tiempo de no disponibilidad de la infraestructura, Disponibilidad del 99.671%.

3.10.2. **TIER II:** Centro de datos Redundante. Los Datacenters de esta categoría tienen redundados sistemas vitales, como la refrigeración, pero cuentan con un único camino de suministro eléctrico. Componentes redundantes (N+1)

Tiene suelos elevados, generadores auxiliares o UPS.

<sup>19</sup> TYCSA, Centro de datos [en línea]. [citado en 07 de Noviembre de 2014]. Disponible en internet: <<http://www.tycsa.info/servicios.html>>



Conectados a una única línea de distribución eléctrica y de refrigeración.

Se trata por tanto de instalaciones con cierto grado de tolerancia a fallos y que permiten algunas operaciones de mantenimiento “on line”.

Disponibilidad del 99.741%.

3.10.3. **TIER III:** Centro de datos Concurrentemente Mantenibles. Un Datacenter TIER III además de cumplir los requisitos de TIER II, tiene niveles importantes de tolerancia a fallos al contar con todos los equipamientos básicos redundados incluido el suministro eléctrico, permitiéndose una configuración Activo / Pasivo.

Todos los servidores deben contar con doble fuente (idealmente) y en principio el Datacenter no requiere paradas para operaciones de mantenimiento básicas.

Componentes redundantes (N+1)

Conectados múltiples líneas de distribución eléctrica y de refrigeración, pero únicamente con una activa.

Es requisito también que pueda realizar el upgrade a TIER IV sin interrupción de servicio.

Disponibilidad del 99.982%.

3.10.4. **TIER IV:** Centro de datos Tolerante a fallos. Esta es la clasificación más exigente en implica cumplir con los requisitos de TIER III además de soportar fallos en cualquier de sus componentes que inhabilite una línea (suministro, refrigeración).

Conectados múltiples líneas de distribución eléctrica y de refrigeración con múltiples componentes redundantes 2 (N+1), ¿Qué significa esto?, que contaremos con 2 líneas de suministro eléctrico, cada una de ellos con redundancia N+1

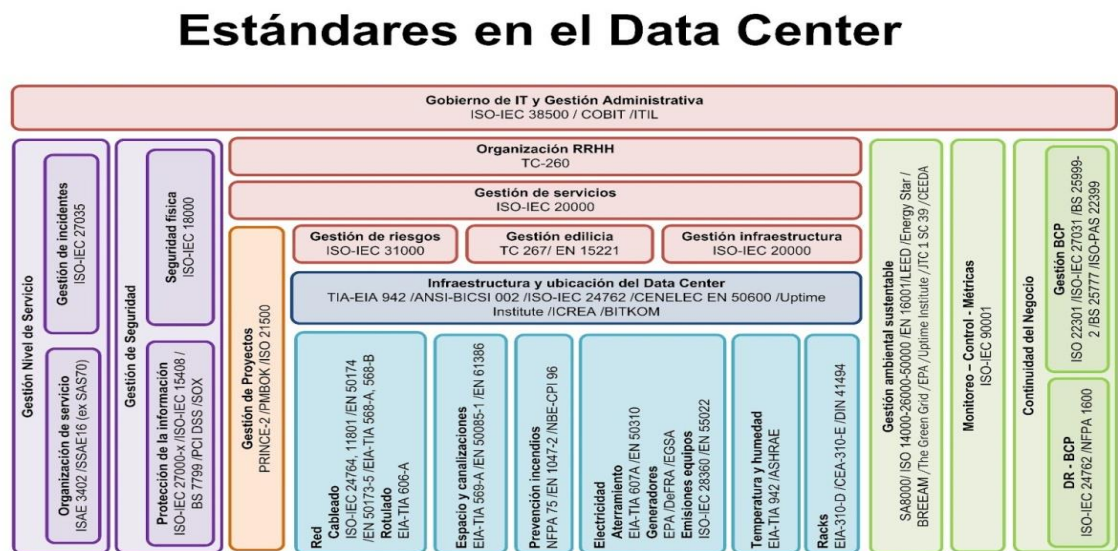
3.10.5. **Estándares en los Data Center<sup>20</sup>.** En la etapa de diseño del Data Center se evalúan cuáles son los estándares que se desearán alcanzar. En ese momento surgen muchas dudas y preguntas relacionadas con el establecimiento de cuáles son los estándares correctos para lograr satisfacer las necesidades del negocio o lo mismo ocurre si se está evaluando un Data Center de un proveedor.

---

<sup>20</sup> Data Centers Hoy, Protección y administración de datos en la empresa [en línea]. [citado en 07 de febrero de 2013]. Disponible en internet: < <http://www.datacentershoy.com/2013/02/estandares-en-el-data-center.html>>

Los cuestionamientos sobre la calidad y los niveles de servicios ofrecidos pueden generar incertidumbre en los clientes. Esta es una tarea dificultosa ya que cumplir con las exigencias de un estándar es muy complejo y costoso. Además en el mercado existen muchos y no es posible cumplir con todos al mismo tiempo ya que tiene objetivos y requerimientos distintos.

FIGURA 4. ESTÁNDARES DE LOS DATACENTER



Los gráficos de burbujas representan subdivisiones por módulos agrupadas por color según el área de aplicación, en letra negrita se pueden el nombre de cada módulo o subdivisión. Los números representan los más estándares o Frameworks más importantes para ese módulo en particular.

Fuente: Datacenter hoy<sup>21</sup>

### 3.11. MARCO GUÍA DE AUDITORÍA

La guía de auditoria consta de una estructura formal, actualmente está en vigencia la norma 19011 de 2012. “Esta Norma Internacional proporciona orientación sobre la gestión de los programas de auditoría, la realización de auditorías internas o externas de sistemas de gestión de la calidad y/o ambiental, así como sobre la competencia y la evaluación de los auditores. Está prevista para aplicarla a una amplia gama de usuarios potenciales incluyendo auditores, organizaciones que estén implementando sistemas de gestión de la calidad y/o ambiental, organizaciones que necesitan realizar auditorías de sistemas de gestión de la calidad y/o ambiental por razones contractuales, y organizaciones involucradas en la certificación o formación de auditores, certificación/registro de sistemas de gestión, acreditación o normalización en el área de la evaluación de la conformidad”

<sup>21</sup> Data Centers Hoy, Protección y administración de datos en la empresa [en línea]. [citado en 07 de febrero de 2013]. Disponible en internet: < <http://www.datacentershoy.com/2013/02/estandares-en-el-data-center.html>>

- a. Gestión de un Programa de Auditoría.
- b. Establecer los objetivos del programa de auditoría.
- c. Establecer el programa de auditoría.
- d. Implementación del programa de auditoría.
- e. Monitoreo del programa de auditoría.
- f. Revisión y mejora del programa de auditoría.
- g. Realización de la auditoría.
- h. Inicio de la auditoría.
- i. Preparación de las actividades de auditoría.
- j. Realización de las actividades de auditoría.
- k. Preparación y distribución del reporte de auditoría.
- l. Finalización de la auditoría.
- m. Realización de auditoría de seguimiento.
- n. Competencia y evaluación de auditores.
- o. Determinación de competencias de auditor para suplir las necesidades del programa de auditoría.
- p. Establecimiento de criterios de evaluación de auditor.

## **4. METODOLOGÍA PROPUESTA**

Este trabajo es de carácter cualitativo, porque parte de un reconocimiento de información relacionado con frameworks y buenas prácticas que estén asociadas con la auditoría en sistemas y la seguridad de la información que actualmente aplican a nivel mundial.

El referente de este trabajo será el estándar ISO 27001 del año 2013 enfocándolo en los Sistemas de Gestión de la Seguridad de la Información (SGSI), en donde se analizarán los componentes o dominios que contiene la norma, y que permitan garantizar la disponibilidad de la información.

Una vez identificados los criterios que permitan garantizar la disponibilidad de la información, se procederá a la construcción de la guía, siguiendo como base la norma ISO 19011 de 2012 la cual establece las directrices para la auditoría en los sistemas de gestión.

### **4.1. ALCANCE DE LA GUÍA DE AUDITORÍA**

El alcance de la guía de auditoría cubrirá los aspectos generales de cualquier auditoría en la nube, sin embargo su foco principal será validar bajo la norma ISO 27001 de 2013, que, el modelo de computación en la nube orientada a la infraestructura como un servicio (IaaS), estén cumpliendo con los requisitos básicos que exige la norma para garantizar la disponibilidad de la información. Como la norma cubre todos los tres pilares de la seguridad (integridad, confidencialidad y disponibilidad) se evaluarán los dominios de la norma para poder identificar cuáles son los más relevantes a la hora de evaluar la disponibilidad.

Basados en esta norma y la norma ISO 27002 de 2013 Se evaluarán los dominios que se tendrán en cuenta a la hora de evaluar los controles que aseguran la disponibilidad de la información en un ambiente Cloud computing con el fin de establecer los puntos a auditar en este tipo de ambientes. Para ello se realizará una matriz analizando cada uno de los dominios, su impacto en la disponibilidad de la información bajo los criterios de continuidad, comunicaciones y nivel de servicio, y detallando que se evaluaría en dicho dominio.

### **4.2. SECTORES Y ÁREAS DE APLICACIÓN DE LA GUÍA DE AUDITORÍA**

El área de aplicación es para todas las organizaciones que requieren llevar a cabo auditorías (Internas o Externas) sobre modelos de infraestructura como un servicio de computación en la nube y/o requieran asegurar la disponibilidad de la infraestructura tecnológica de estas. Así mismo se espera que la guía sirva de apoyo a la adquisición de servicios Cloud al momento de evaluar y validar un proveedor de este tipo de servicios.

### 4.3. ANÁLISIS DE RIESGOS

Los sistemas tradicionales se encuentran protegidos detrás de firewalls, NATs, VPNs, y un conjunto de restricciones, de modo que los atacantes deber realizar una exhaustiva labor de inteligencia para saber que ellos existen dice Greg Day – Analista de seguridad de McAfee. Los servicios en la nube en cambio son altamente visibles y están diseñados para ser accedidos desde cualquier parte por cualquier persona, un gran blanco en cuestión.

Hay varias áreas de preocupación en cuanto a los riesgos de cloud computing y la seguridad:

- **Disponibilidad de la red:** sólo se puede obtener el valor de cloud computing cuando la conectividad de red y el ancho de banda de satisfacen las necesidades mínimas. La nube debe estar disponible siempre que lo necesite. De lo contrario, las consecuencias no son diferentes que un ataque de denegación de servicio.
- **Viabilidad de proveedor de la nube:** debido a que los proveedores de nube son relativamente nuevos para el negocio, hay preguntas sobre su viabilidad y compromiso. Esta preocupación se profundiza cuando un proveedor requiere los inquilinos utilizar interfaces patentadas, conducen a inquilinos en bloqueo.
- **Recuperación ante desastres y continuidad del negocio:** los inquilinos y los usuarios requieren que sus operaciones y servicios continuará si el entorno de producción del proveedor de la nube está sujeto a un desastre de confianza.
- **Incidentes de seguridad:** el proveedor debe informar a los inquilinos y los usuarios de cualquier infracción de seguridad. Los inquilinos o los usuarios pueden requerir compatibilidad del proveedor para responder a la auditoría o resultados de la evaluación. También, un proveedor puede no ofrecer apoyo suficiente a los inquilinos o los usuarios para resolver las investigaciones.
- **Transparencia:** cuando un proveedor de la nube no expone los detalles de su propia directiva interna o la tecnología, los inquilinos o los usuarios deben confiar en las reclamaciones de seguridad del proveedor. Los inquilinos y los usuarios todavía pueden requerir alguna transparencia por proveedores como cómo administran la seguridad de la nube, privacidad e incidentes de seguridad.
- **Pérdida de Control físico:** porque los inquilinos y los usuarios pierden control físico sobre sus datos y aplicaciones, esto da lugar a una gama de preocupaciones:

Por tanto, es recomendable evaluar las consecuencias a nivel de seguridad antes de empezar cualquier proceso de migración/implantación de un sistema en la nube. En el desarrollo de la guía y sus anexos tendremos encuentra estos puntos para realizar preguntas específicas sobre las mismas.

#### **4.4. PARTES INTERESADAS**

Personas o entidades que tienen contratado servicios de computación en la nube orientados a infraestructura y requieren evaluar la disponibilidad de este servicio.

## **5. CARACTERIZACIÓN DE DOMINIOS NORMA ISO 27001**

La norma ISO 27001:2013 suministra requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de seguridad de la información (SGSI) en cualquier tipo de organización, independientemente de su tipo, tamaño o naturaleza; el SGSI preserva los pilares de la seguridad (confidencialidad, integridad y disponibilidad) mediante la gestión de riesgos y la aplicación de controles para mitigarlos.

Descriptivo de los dominios seleccionados:

La matriz del Anexo A – Caracterización de dominios norma ISO 27001, caracteriza los dominios que son primordiales a la hora de evaluar el aseguramiento de la disponibilidad de la información. Cada dominio fue evaluado bajo tres criterios (comunicaciones, continuidad y nivel de servicio); Los tres criterios fueron tomados como referente, con base en buenas prácticas de auditoría, profesionales y docentes de auditoría y a lo aprendido durante el transcurso de la especialización en auditoría de sistemas.

Una vez obtenidos los dominios relevantes a la hora de evaluar la disponibilidad, se desglosan los puntos a evaluar, esto se realiza analizando en detalle lo establecido para cada dominio en la norma ISO 27002 de 2013.

El resultado final de este proceso es una lista de chequeo y verificación de lo que se debería evaluar en cada uno de los dominios seleccionados.

## **6. ESTRUCTURACIÓN DE LA GUÍA DE AUDITORÍA**

Como punto de partida se toma la Norma 19011 de 2012, como referente para estructurar la guía de auditoría “Guía de auditoría para evaluar el aseguramiento de la disponibilidad de la información en un ambiente Cloud Computing IaaS, bajo la norma ISO 27001 de 2013”. Para cubrir el alcance de este proyecto se tomarán los ítems de la norma (Inicio de la auditoría, Preparación de las actividades de auditoría, Realización de las actividades de auditoría, Preparación y distribución del reporte de auditoría y Finalización de la auditoría).

La guía de auditoría estará compuesta por las siguientes partes:

- Presentación.
- Generalidades.
- Normas de auditoría.
- Definiciones.
- Componentes básicos de la auditoría.
- Entidades externas o regulación.
- Fase de auditoría.
- Inicio de la auditoría.
- Preparación de actividades de auditoría.
- Realización de las actividades de auditoría.
- Preparación y distribución del informe de auditoría.
- Finalización de la auditoría.

Teniendo en cuenta que la finalidad de la guía de auditoría es evaluar el aseguramiento de la disponibilidad de la información, se hará referencia a la caracterización de los dominios de la norma ISO 27001 de 2013 realizada en el punto anterior. Esta lista de chequeo junto con otros formatos usados en las buenas prácticas de auditoría, se usarán como apoyo al proceso de auditoría que propone la guía desarrollada.

Los formatos anexos a la guía de auditoría son:

- ANEXO A - FORMATO FAMILIARIZACIÓN O ENTENDIMIENTO
- ANEXO B - FORMATO ACTA DE INICIO
- ANEXO C - FORMATO REQUERIMIENTOS
- ANEXO D - FORMATO DE SEGUIMIENTO
- ANEXO E - FORMATO INFORME
- ANEXO F - FORMATO ACTA DE CIERRE
- ANEXO G - LISTA DE CUESTIONARIO DE ISO 27001
- ANEXO H - LISTA DE CUESTIONARIO DATA CENTER TIER



## **7. VALIDACIÓN DE GUÍA DE AUDITORÍA**

Una vez desarrollada la guía de auditoría para evaluar el aseguramiento de la disponibilidad de la información en un ambiente Cloud Computing IaaS, bajo la norma ISO 27001 de 2013, es enviada a un grupo de expertos, conocedores en las áreas de auditoría y seguridad de la información.

A este grupo de expertos se les envió vía correo electrónico, la guía, una invitación formal (Anexo C) y un cuestionario (Anexo D) cuyo objetivo final es validar la guía en su estructura y aplicabilidad.

Las observaciones y recomendaciones dadas por los expertos, fueron implementadas como mejoras a la guía, antes de ser entregada formalmente.

## **8. CONCLUSIONES**

La auditoría tradicional, es aplicable a la auditoría en la nube, siempre y cuando se evalúe bajo un estándar o normatividad.

En un ambiente Cloud computing IaaS (Infraestructura como un Servicios), la disponibilidad de la información, evaluada bajo la norma ISO 27001 de 2013 debe tener en cuenta criterios primordiales al momento de garantizar el servicios y la operatividad.

Con la caracterización de los dominios, se obtuvo una lista de chequeo con los principales objetivos de control que impactan la disponibilidad de la información. Así mismo se implementaron preguntas orientadas a conocer el nivel de confianza en el cual se encuentra el servicio Cloud (Niveles Tier)

Las fases de la guía de auditoría para valuar un ambiente en la nube, están basadas en la norma ISO 19011 de 2012.

Se concluye que es importante contar con formatos de que apoyen el proceso de auditoría, con el fin de brindar un mayor entendimiento y detalle de cada ítem a solicitar, realizar o generar. Además que permite hacer seguimiento al proceso o ente auditado.

Finalmente la validación de la guía por medio de un grupo de expertos, permitió enriquecer la guía y enfocarla hacia el objetivo auditable (Cloud IaaS)

Se espera que la guía sea un valioso aporte para posteriores proyectos relacionados con seguridad y/o auditoría en ambientes Cloud.

## BIBLIOGRAFÍA

ARIEL Alonso, Cloud Computing [en línea]. [Citado el 25 de Agosto de 2014]. Disponible en internet: < <http://cloudcomputinguq.wordpress.com/casos-de-exito/>>

BOXBYTE, El origen del Cómputo en la nube [en línea]. [Citado en 22 de Agosto de 2014]. Disponible en internet: <<http://www.fayerwayer.com/2012/01/el-origen-de-el-computo-en-la-nube/>>

BSA - The Software Alliance. Global Cloud Computing Scorecard, [en línea]. [Citado 4 octubre de 2014]. Disponible en internet en internet: <<http://www.cloudempresarial.com/tweets/5-estadisticas-del-cloudcomputing-que-usted-puede-encontrar-sorprendentes/>>

BSA - The Software Alliance. Global Cloud Computing Scorecard, [en línea]. [Citado 4 octubre de 2014]. Disponible en internet: <[http://cloudscorecard.bsa.org/2013/assets/PDFs/BSA\\_GlobalCloudScorecard2013\\_Spanish.pdf](http://cloudscorecard.bsa.org/2013/assets/PDFs/BSA_GlobalCloudScorecard2013_Spanish.pdf)>

BSA. Estudio sobre puntuación global de computación en la nube BSA 2013. [en línea] EE.UU: BSA [citado en 12 de Agosto de 2014]. Disponible en internet: <[http://cloudscorecard.bsa.org/2013/assets/PDFs/BSA\\_GlobalCloudScorecard2013\\_Spanish.pdf](http://cloudscorecard.bsa.org/2013/assets/PDFs/BSA_GlobalCloudScorecard2013_Spanish.pdf)>

CINTEL. Centro de Investigación y Desarrollo en Tecnologías de la Información y las Comunicaciones [en línea]. [Citado 4 octubre de 2014]. Disponible en internet: <<http://cintel.org.co/wp-content/uploads/2013/06/resultados-del-estudio.pdf>>

CLOUD COMPUTING, Computación en nube [en línea]. [Citado en 10 de Agosto de 2014]. Disponible en internet: <<http://www.computacionennube.org/13/tipos-de-nube/>>

Cloud Security Alliance, Security Guidance for critical areas of focus Cloud computing V2.1 [en línea]. EE.UU: NIST [citado en 12 de Agosto de 2014]. Disponible en internet: <<https://cloudsecurityalliance.org/guidance/csaguide.pdf>>

COLOBRAN HUGUET Miguel, Administración de sistemas operativos en red: Administración de servidores. Barcelona: Editorial UOC, 2008. 37 p. ISBN: 978-84-9788-760-1

CSA, Security Guidance for Critical Areas of Focus in Cloud Computing V2.1 [en línea]. [citado 8 Agosto de 2014] Disponible en internet: <<http://www.cloudsecurityalliance.org/guidance/csaguide.pdf>>

Data Centers Hoy, Protección y administración de datos en la empresa [en línea]. [Citado en 07 de febrero de 2013]. Disponible en internet: <

<http://www.datacentershoy.com/2013/02/estandares-en-el-data-center.html>>

Data Centers Hoy, Protección y administración de datos en la empresa [en línea]. [Citado en 07 de febrero de 2013]. Disponible en internet: <<http://www.datacentershoy.com/2013/02/estandares-en-el-data-center.html>>

GOOGLE, The Google File System [en línea]. [Citado en 15 de Septiembre de 2014]. Disponible en internet: <<http://static.googleusercontent.com/media/research.google.com/es-419/archive/gfs-sosp2003.pdf> >

IBM, Cloud Computing Use Cases Whitepaper [en línea]. IBM [citado en 20 de septiembre de 2014]. Disponible en internet: <<http://www.ibm.com/developerworks/ssa/cloud/library/cl-rev2sla.html>>

INTERNAUTE, Cloud Computing, [en línea]. [Citado 22 de agosto de 2014]. Disponible en internet: <<http://www.interoute.es/>>

NIST, The NIST definition of Cloud computing, Special Publication 800-145 [en línea]. [Citado 12 de agosto de 2014]. Disponible en internet: <<http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>>

OBSERVATORIO TECNOLOGICO, Seguridad informática [en línea]. España: Elvira Mifsud [citado 12 Octubre de 2014]. Disponible en internet: <<http://recursostic.educacion.es/observatorio/web/ca/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=1>>

SONDA Cloud Computing, Informes Digitales [en línea]. [Citado 24 julio 2014]. Disponible en internet: <<http://cloudempresarial.com/tweets/5-estadisticas-del-cloudcomputing-que-usted-puede-encontrar-sorprendentes/> >

TIA TR-42 Telecommunications Cabling Systems engineering committee recently released a second addendum to the TIA-942 Data Centers standard [en línea]. [Citado en 18 de septiembre de 2014]. Disponible e internet < <http://www.tiaenlinea.org/news-media/news-articles/tia-942-data-center-cabling-standard-amended> >

TYCSA, Centro de datos [en línea]. [Citado en 07 de Noviembre de 2014]. Disponible en internet: <http://www.tycsa.info/servicios.html>

## **ANEXO A - CARACTERIZACIÓN DE LA NORMA ISO 27001**

Ver adjunto en carpeta ANEXOS/ Caracterización de la norma ISO 27001 DE 2013.xls

**ANEXO B - GUÍA DE AUDITORÍA PARA EVALUAR EL ASEGURAMIENTO DE  
LA DISPONIBILIDAD EN UN AMBIENTE CLOUD COMPUTING IAAS BAJO LA  
NORMA ISO 27001 DE 2013**

Ver adjunto en carpeta ANEXOS/ANEXO B - GUIA DE AUDITORIA CLOUD  
COMPUTING IAAS.docx

## ANEXO C - CARTA INVITACIÓN A EVALUACIÓN DE GUÍA

Bogotá D.C, 13 de Noviembre de 2014

Ingeniero  
**XXXXXXX**  
Profesor postgrado Auditoria de Sistemas  
**UNIVERSIDAD CATOLICA**  
Bogotá D. C.

**REFERENCIA: Apoyo en la revisión de la “GUIA DE AUDITORIA PARA EVALUAR EL ASEGURAMIENTO DE LA DISPONIBILIDAD DE LA INFORMACIÓN EN UN AMBIENTE CLOUD COMPUTING IAAS, BAJO LA NORMA ISO 270001 DE 2013”**

Apreciado Ingeniero:

Reciba un cordial y atento saludo, deseándole éxitos en la gestión como educador en la Universidad Católica.

El grupo de estudiantes de la especialización de Auditoria de Sistemas de la Universidad Católica de Colombia, conformado por los estudiantes: Marien Hernández Vega, Johan Sebastián Murcia y Cristian Giovanni Toro Sánchez; nos encontramos actualmente realizando el proyecto de grado y que será sustentado en la primera semana de diciembre del 2014.

Por lo cual extendemos la invitación formal para que nos aporte con sus conocimientos profesionales y académicos en la revisión de la guía de auditoría para evaluar la seguridad de la información en términos de disponibilidad en un ambiente Cloud Computing IaaS bajo la norma ISO 27001 de 2013

Anexamos documento borrador de la guía.

En espera de su respuesta,

Cordialmente,

<u>Marien Hernández Vega.</u>	<u>Johan Sebastián Murcia.</u>	<u>Cristian G. Toro Sánchez</u>
Estudiante	Estudiante	Estudiante

**ANEXO D – VALIDACIÓN DE LA GUÍA DE AUDITORIA PARA EVALUAR EL  
ASEGURAMIENTO DE LA DISPONIBILIDAD EN UN AMBIENTE CLOUD  
COMPUTING IAAS BAJO LA NORMA ISO 27001 DE 2013**

Nombre: \_\_\_\_\_

Profesión: \_\_\_\_\_

Fecha: \_\_\_\_\_

<b>PREGUNTAS</b>	<b>SI/NO</b>
¿La estructura que tiene la guía de auditoría, cumple con las fases y requisitos para cumplir con su finalidad?	
¿La guía de auditoría está orientada a evaluar la disponibilidad de la información en un ambiente Cloud Computing IaaS?	
¿La guía de auditoría está estructurada bajo la norma ISO 19011 de 2012?	
¿Los dominios de la norma ISO 27001 DE 2013, tenidos en cuenta en la guía de auditoría, son suficientes para evaluar la disponibilidad de la información?	
¿Los formatos anexos a la guía de auditoría, son suficientes en un proceso de auditoría?	
Si la finalidad de la guía es evaluar la disponibilidad de la información en un ambiente Cloud IaaS, ¿la guía proporciona el paso a paso para su realización?	
¿Qué recomendaciones daría para mejorar la guía de auditoría?	
¿Qué recomendaciones haría frente a los anexos de la guía de auditoría?	
De 1 a 5, siendo 5 la mejor puntuación, ¿En qué nivel califica usted la guía de auditoría?	