

FACULTAD DE INGENIERÍA

ESCUELA DE SISTEMAS

DISERTACIÓN DE GRADO PREVIA LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS Y COMPUTACIÓN

TEMA:

IMPLEMENTACIÓN DE UN ESQUEMA DE SEGURIDAD EN MICROSOFT AZURE PARA CLOUD COMPUTING, APLICANDO DOS METODOLOGÍAS PREVIAS SU EVALUACIÓN, CASO DE ESTUDIO EMPRESA MICROSOFT DEL ECUADOR

DIRECTOR:

ING. ANDRÉS JIMENEZ

AUTOR:

THALIA ALEJANDRA LOZADA ARELLANO

QUITO – 2018

Declaratoria de Responsabilidad

Los conceptos desarrollados, análisis realizados y las conclusiones del presente trabajo, son de exclusiva responsabilidad del autor

Thalía Alejandra Lozada Arellano

Agradecimiento

Agradezco a Dios, por guiarme y darme la fuerza para concluir con unas etapas más en mi vida llena de alegrías, difíciles y grandes momentos guiándome y brindándome su bendición a cada momento para poder seguir por el sendero correcto y del éxito.

Agradezco a mi universidad la Pontificia Universidad Católica del Ecuador por las enseñanzas brindadas, y a cada uno de mis profesores que me enseñaron la parte teórica y práctica de nuestra carrera, así como el don de gente que se llevar a lo largo de nuestra profesión.

Agradezco a mi director Ing. Andrés Jiménez por su apoyo, y colaboración para la culminación de mi tesis por medio de su retroalimentación y pautas.

Agradezco al Ing. Beatriz Campos e Ing. Oswaldo Espinoza por su apoyo, y colaboración para la culminación de mi tesis por medio de su retroalimentación.

Agradezco a Microsoft Ecuador, empresa que me ayudado alrededor de 3 años con conocimiento y grandes experiencias, ellos han sido una gran escuela para mí, también por el apoyo en el desarrollo de esta tesis poniendo a disposición todo el material requerido y necesitado.

Agradezco a mi familia por comprenderme, amarme y luchar conmigo por obtener esta anhelada meta.

Dedicatoria

Esta disertación se lo dedico a:

A mi madre Mercedes, por caminar de mi mano y apoyarme en toda esta etapa de mi vida formando desde pequeña hasta hoy en día cimientos de amor, respeto, lealtad, compresión y paciencia hacia mí, gracias por todo tu amor incondicional y lucha constante, sin ti no lo hubiera logrado.

A mi hermana Emilia, tu corazón noble y apoyo en cada momento como mi mejor amiga, hace que yo vea el mundo diferente, a quien deseo verla a futuro como una gran Doctora y cumpliendo sus grandes metas.

A mi abuelita Rosario por la gran paciencia, cuidado y consejos alrededor de toda mi vida, así como también el apoyo incondicional a lo largo de esta gran meta.

Mis tres personas más importantes en la vida y por ustedes todo, las amo mucho y son mi tesoro más preciado en esta vida.

Thalía Lozada

Resumen

Hoy en día los activos de información son de gran importancia en cualquier organización y son parte de la toma de decisiones, predicciones y optimización de la misma, en efecto mantenerla segura es un reto para muchos.

Para proteger adecuadamente dicha información, las organizaciones e individuos necesitan primero entender qué información poseen y lo valiosos que son. Este entendimiento debe estar claro cuando la información se traslada a la nube por completo, donde más de un usuario pueda acceder a ella, esto incluye personal de las empresas proveedores de servicios en la nube y terceros.

Actualmente para mantener y garantizar integridad, confidencialidad y disponibilidad se cuenta con herramientas, estándares y metodologías para la transferencia, procesamiento y almacenamiento en tiempo real de la información.

Esta disertación presenta la implementación demostrativa para el proceso de movimientos y clientes otorgado para el caso de estudio de Microsoft del Ecuador, utilizando Microsoft Azure. Se utilizará un sistema de inteligencia de negocios con dos metodologías y estándares de seguridad para reducir el riesgo de amenazas y vulnerabilidades previamente analizadas, manejando su correspondiente documentación, controles de mitigación de riesgo y buenas prácticas. Además, se podrá visualizar la información de auditoría y clientes a través de herramientas de despliegue como son: Power BI y Excel.

El beneficio de dicha implementación demostrativa de un esquema de seguridad en la nube será:

1. La prevención de amenazas y el cifrado de datos en tiempo real se ajustará a cualquier organización que cuente con características y activos similares.
2. Visualización personalizada de reportes partiendo de información limpia, confiable y disponible.

Tabla de Contenidos

Declaratoria de Responsabilidad 2

Agradecimiento 3

Dedicatoria 4

Resumen 5

CAPÍTULO I: INVESTIGACIÓN SOBRE EL ESTADO DEL ARTE DE CLOUD COMPUTING EN EL ECUADOR Y EL MUNDO 10

1.1 Introducción a Cloud Computing 10
1.2 Historia Cloud Computing 11
1.2.1 Concepto Cloud Computing 14
1.2.2 Proveedores extranjeros 16
1.2.3 Proveedores Nacionales 17
1.2.4 Comparativo de servicios de proveedores nacionales y extranjeros 21
1.2.5 Nivel de Adopción Cloud Computing 23
1.2.6 Beneficios Cloud Computing 28
1.2.7 Limitaciones Cloud Computing 29
1.3 Principales metodologías de seguridad en la nube 30
1.4 Análisis de seguridad de cada una de las metodologías. 36
1.5 Selección de las dos mejores metodologías para realizar el diseño de esquema de seguridad. 38

CAPÍTULO II: ANÁLISIS COMPARATIVO SOBRE SEGURIDAD 40

2.1 Preocupaciones al momento de adoptar Cloud Computing 40
2.1.1 Seguridad de la información 40
2.1.2 Privacidad 42
2.1.3 Confiabilidad 43
2.2 Seguridad en Cloud Computing y comparación 44

CAPÍTULO III: IMPLEMENTACIÓN DE ESQUEMAS DE SEGURIDAD 54

3.1 Sistema de Gestión de Seguridad de la Información (SGSI) 54
3.2 Implementación de aplicativos en la nube utilizando un SGSI 60
3.2.1 Administración de la información durante la implementación de aplicativos en la nube 61
3.3 Metodologías de cifrado 62
3.3.1 Algoritmos simétricos 63
3.3.2 Algoritmos asimétricos 66

3.3.3 Algoritmos Hash 67

CAPÍTULO IV: DISEÑO E IMPLEMENTACIÓN DE ESQUEMA DE SEGURIDAD EN LA NUBE MICROSOFT AZURE 70
4.1 Diseño del esquema de seguridad 70
4.1.1 Planificar 70
4.1.2 Análisis y Evaluación del Riesgo 75
4.1.3 Seguridad de la información en los activos de la compañía seleccionada 82
4.1.3.1 Asignación de roles y responsabilidades 82
4.1.3.2 Eliminación de roles y responsabilidades 83
4.1.3.3 Posibilidad de Ocurrencia del Riesgo 85
4.1.3.4 Tratamiento del riesgo 86
4.1.3.5 Enunciado de aplicabilidad 86
4.1.4 Hacer 87
4.1.5 Verificar 92
4.2 Implementación de Esquema de Seguridad 97
4.2.1 Actuar 97
4.3 Muestra de reportes finales del proceso seleccionado 109

CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES 113
5.1 Conclusiones 113
5.2 Recomendaciones 114

BIBLIOGRAFÍA 116

ANEXOS 119
Anexo 1: 119
Anexo 2: 142
Anexo 3: GLOSARIO 148

Índice de Gráficos

Ilustración 1: Perfil de encuestados de CloudView 2016; por cargo 24
Ilustración 2: Perfil de encuestados de CloudView 2016; por zona geográfica 25
Ilustración 3: Análisis de adopción de nube en CloudView 2016 25
Ilustración 4: Análisis de adopción de nube en CloudView 2016 26
Ilustración 5: Análisis de adopción de nube pública en CloudView 2016 26
Ilustración 6: Análisis de adopción de nube privada en CloudView 2016 27

Ilustración 7: Servicios HIPAA 33
Ilustración 8: Pasos a seguir para implementación de estándar CPS 34
Ilustración 9: Modelo preliminar de diseño de esquema de seguridad 39
Ilustración 11: Plan de acción de seguridad 45
Ilustración 12: AWS análisis de seguridad en servicios Cloud Computing 52
Ilustración 13: Microsoft Azure análisis de seguridad en servicios Cloud Computing 52
Ilustración 14: Google Cloud análisis de seguridad en servicios Cloud Computing 53
Ilustración 10: Seguridad en la nube 57
Ilustración 16: Cuatro tipos de documentación en el Modelo de SGSI 58
Ilustración 17: Modelo de Sistema de Seguridad de la Información 59
Ilustración 15: Ciclo de vida de seguridad de la información antes, durante y después de la migración a la nube 61
Ilustración 18: Organigrama de la compañía 72
Ilustración 19: Metodología de las Elipses 73
Ilustración 20: Análisis de Riesgos 75
Ilustración 21: Metodología para el Análisis y Evaluación del Riesgo 76
Ilustración 22: Proceso de reclutamiento (asignación de roles y responsabilidades) 83
Ilustración 23: Baja de usuarios en la compañía 84
Ilustración 24: Proceso de Planificación SGSI 87
Ilustración 25: Proceso de Hacer en SGSI 88
Ilustración 26: Diseño de Arquitectura de Implementación en la nube 88
Ilustración 27: Proceso de Verificación SGSI 90
Ilustración 28: Proceso de Actuar/Final en SGSI 90
Ilustración 29: Diseño de esquema de información de proceso seleccionado 91
Ilustración 30: Diseño de proceso de Implementación de Tratamiento de Riesgo en Microsoft Azure 93
Ilustración 31: Diseño a detalle de Arquitectura de Implementación en la nube 95
Ilustración 32: Diseño a detalle de esquema de información de proceso seleccionado 97
Ilustración 33: Dashboard en Microsoft Azure 99
Ilustración 34: Autentificación y acceso SQL Azure (sin registro previo de IP) 100
Ilustración 35: Registros de Clientes IP para acceso autorizado 101
Ilustración 36: Autentificación y registro de acceso a Visual Studio Business Intelligence 102
Ilustración 37: Acceso no registrado en la base de datos de IPs en el caso de la herramienta Visual Studio Business Intelligence 103
Ilustración 38: Test de conexión a bases de datos en la nube para proceso ETL 104
Ilustración 39: Pre visualización de información en carga ETL 104
Ilustración 40: Diseño de Carga ETL 105
Ilustración 41: Proceso ETL desarrollado en Data Factory para carga de datos en ODS 105
Ilustración 42: Carga de Datos de Datawarehouse por medio de ETL en Data Factory 106
Ilustración 43: Despliegue de datos en Datawarehouse utilizando Data Factory 106

Ilustración 44: Visualización de Audit Logs en Azure Storage Explorer _____ 107
Ilustración 45: Correo de alertas para detección de amenazas _____ 108
Ilustración 46: Jerarquía de cifrado de datos _____ 109
Ilustración 47: Reporte de Logs almacenados en Hadoop por cada base de datos migrada _____ 110
Ilustración 48: Reporte de Logs almacenados en Hadoop por cada base de datos migrada en base a la fecha_____ 111
Ilustración 49: Reportes orientados a la información entregada por la compañía _____ 112

Índice de Tablas

Tabla 1: Cuadro comparativo de proveedores nacionales _____ 21
Tabla 2: Cuadro Comparativo de Proveedores Extranjeros _____ 22
Tabla 3: Cuadro de especificación de funciones y usuarios SOC 1, 2, 3 _____ 35
Tabla 4: Tabla Comparativa de Metodologías de Seguridad en la nube_____ 37
Tabla 5: Tabla comparativa de planes de seguridad en la nube _____ 49
Tabla 6: Tabla Comparativa de Acuerdos y Regulaciones de nube _____ 51
Tabla 7: Identificación y Evaluación de Activos _____ 78
Tabla 8: Análisis y Evaluación de Riesgo iniciales _____ 81

Capítulo I: Investigación sobre el estado del arte de Cloud Computing en el Ecuador y el mundo

1.1 Introducción a Cloud Computing

La computación en la nube (Cloud Computing) se la conoce desde mediados del siglo XX. Es una evolución de la adopción de virtualización, arquitectura orientada a servicios y la prestación de los mismos y su idea a un principio era que los usuarios finales ya no necesitaban conocer acerca del tema o el control sobre la infraestructura montada en la nube que los apoya.

Poco a poco dichos usuarios tenían mayores necesidades a las implementadas tales como: escalabilidad, respuesta inmediata, procesos óptimos, entre otros. Algunas de las funcionalidades no se encontraban desarrolladas, los distintos proveedores lo fueron haciendo posible ofertando distintos planes, para usuarios personales o empresas.

El 87% de los usuarios de la nube han adoptado algunas capacidades para una estrategia de nube híbrida, un aumento del 17% en comparación con 2016. Muchas empresas realizaron estudios para conocer detalladamente sobre lo que estaba sucediendo tales como: DELL, Cisco, IBM, etc.[1]

"Dell reveló en su estudio denominado **Global Technology Adoption Index 2015** (GTAI 2015), que las organizaciones que utilizan activamente tecnologías de Cloud Computing, movilidad, Big Data o seguridad están experimentando tasas de crecimiento de ingresos de hasta un 53% superiores a las que no han invertido en estas tecnologías." [2]

A pesar de este fuerte vínculo entre el uso de las nuevas tecnologías, optimización, crecimiento de los ingresos y ahorro de costos, existen diferentes brechas como la seguridad y miedo a la violación de datos y disponibilidad a un cien por ciento entre los mayormente sobresalientes.

Sin embargo, algunos ejecutivos de TI siguen siendo escépticos de que los beneficios de utilizar la nube y su enfoque prioritario son los riesgos anteriormente mencionados que

[1] Michael Shirer, Benjamin McGrath. (2017). IDC's Latest CloudView Study Reveals the Top Three Drivers of Cloud Adoption. 2017, de IDC Sitio web: https://www.idc.com/getdoc.jsp?containerId=prUS42878417

[2] DELL. (2015). Global Technology Adoption Index 2015. 2016, de DELL Sitio web: http://en.community.dell.com/dell-blogs/direct2dell/b/direct2dell/archive/2015/10/08/global-technology-adoption-index-2015

involucra. Algunas compañías y personas temen que la comunicación y envío de información a través de una red pública sean vulnerables a los ataques cibernéticos.
Otros se preocupan de que los proveedores que ofrecen la misma infraestructura a múltiples clientes en múltiples ubicaciones no podrán mantener confidencialidad segregada. Es por el hecho de que la información administrada a través del almacenamiento en servidores geolocalizados en distintos lugares alrededor del mundo se exponga a diferentes requerimientos y reglamentos con los cuales no se encuentra familiarizados.

De acuerdo al libro de la compañía auditora EY denominado **"Building trust in the cloud"** se debe desarrollar una modelo de nube confiable para evaluar, monitorear, mejorar y certificar cumpliendo estándares para que los profesionales de TI puedan convertir el miedo de la nube en una oportunidad para dirigir cada vez seguridad y desafíos de seguridad mucho más complejos.

En resumen, a medida que la computación en nube entra en su segunda década de vida, su prevalencia está aumentando hasta el punto en que su enfoque tiene gran expectativa en el área de tecnología. A pesar de su longevidad, la computación en nube sufre en silencio desde la confusión y preocupaciones no técnicas, por ejemplo, el costo y la gobernabilidad continúan confundiendo las opiniones y enfoques de los directores de TI, arquitectos y líderes de la nube.

Los ejecutivos de TI necesitan aprender cómo establecer un ambiente seguro y confiable cambiando el enfoque hacia la construcción de un ecosistema de nube de confianza.

Es un tema muy amplio y está afectando de a poco en prácticamente todos los aspectos de TI, convirtiendo a la nube en un vehículo en donde gran parte de lo que se describe, es como el futuro de las tecnologías, se encontrará ahí tales como: Negocios digitales, internet de las cosas (IoT), aprendizaje automático, algorítmica, inteligencia de negocios, bots, etc.[3]

1.2 Historia Cloud Computing

Su historia según diferentes investigaciones remonta en 1961 cuando John McCarthy, profesor de ciencia de computación en la Universidad de Stanford, mencionó en una conferencia "Algún día la información podría ser organizada como un servicio público", dicha conferencia fue para celebrar los 100 años del MIT (Massachusetts Institute of Technology). [4]

[3] David Mitchell Smith. (Abril 2016). Cloud Computing Primer for 2016. Gartner, 1, 12. 2016

[4] David López Jiménez. (2013). Cloud Computing Analyzed From the Spanish Legal System. 2016, de Revista de derecho (Valparaíso) Sitio web: http://www.scielo.cl/scielo.php?pid=S0718-68512013000100021&script=sci_arttext

Lo mencionado anteriormente comenzó a tener forma y convertirse poco a poco en realidad alrededor de 1960 a 1970, donde el concepto de virtualización era posible debido a que uno o más sistemas operativos se podían ejecutar simultáneamente, varias empresas proporcionaban recursos compartidos que incluían: paquetes de programas informáticos, editores de textos, impresión y almacenamiento.

Y en el año 1990 las compañías de telecomunicaciones ofrecían virtualizaciones de redes privadas, pero a precio reducido evitando la construcción de una estructura física.

Uno de los primeros hitos en la historia de la nube fue la llegada de Salesforce.com en 1999, que fue pionera en el concepto de la entrega de aplicaciones empresariales a través de un sitio web sencillo. Dicha firma de servicios allanó el camino para el especialista y las empresas de software de comunicación para entregar aplicaciones en internet.

En 1996 Amazon una empresa fundada en Seattle, USA, comenzó con el comercio de libros por internet iniciando con los primeros desarrollos en la nube, para más adelante con Amazon Web Services en 2002 proporcionar un conjunto de servicios basados en la nube, incluyendo el almacenamiento, la computación e inteligencia artificial, a través de la Amazon Mechanical Turk. La plataforma permite que los solicitantes ingresen al sistema unidades de trabajos (HIT, “Human Intelligence Tasks” o “Tareas de Inteligencia Humana”) y los trabajadores “Turkers” pueden consultar dichos trabajos y finalizarlos. Éstos, a cambio, reciben una recompensa económica impuesta por el solicitante.

Luego en 2006, Amazon lanzó Elastic Compute Cloud (EC2) como un servicio web comercial que permitía a las pequeñas compañías e individuos alquilar computadoras en los cuales se ejecutaban sus propias aplicaciones informáticas.

"Amazon EC2 / S3 fue primer servicio de la infraestructura de computación en la nube ampliamente accesible", dijo Jeremy Allaire, CEO de Brightcove, que ofrece plataforma SaaS de vídeo en línea a las estaciones de televisión de Reino Unido y periódicos.

Otro hito importante se produjo en 2009, con la llegada del Web 2.0; Google y otros comenzaron a ofrecer aplicaciones empresariales basadas en el uso del navegador, a través de servicios tales como Google Apps.

"La contribución más importante a la computación en nube ha sido la aparición de "aplicaciones asesinas" (se caracteriza porque reemplaza total a parcialmente a otro servicio tradicional) de las principales compañías de la tecnología tales como: Microsoft,

Amazon, Salesforce.com y Google; cuando las empresas más conocidas ofrecen servicios de una manera confiable y fácil de consumir".[5]

Otros factores clave que se encuentran habilitados en el Cloud Computing para su evolución incluyen la maduración de la tecnología de virtualización, el desarrollo de banda ancha universal de alta velocidad, y los estándares de interoperabilidad de software universal, opinión realizada por Jamie Turner pionera del marketing en la nube. Turner además añadió: "A medida que la nube se extiende su alcance va más allá de una adopción temprana de repositorios en la nube tales como: Dropbox, Google Docs, entre otros. Lo que permite sólo empezar a imaginar su ámbito y afirmar que casi cualquier cosa puede ser entregado desde la nube."[6]

Poco a poco las necesidades de los usuarios fueron mayores y los proveedores de nube comenzaron a ofrecer servicios según sus requerimientos, presupuesto, negocios y uso; los proveedores inicialmente ofrecen **tres distintas clases de nube** para comenzar nuestro diseño e implementación de aplicaciones o servicios a desplegar. Estos tres tipos difieren en la cantidad de control que se tiene sobre la información, como también el control por parte del proveedor en dicha información.

Brevemente a continuación detallaremos su definición por cada clase:

SaaS: Por medio de un proveedor se adquiere una o varias aplicaciones las cuales sus clientes pueden administrarlas ya sea como un servicio bajo demanda, a través de una suscripción, en un modelo de "pago por uso" o sin cargo cuando hay oportunidad de generar ingresos por medio de un tercero, como por ejemplo en las ventas de anuncio.

PaaS: Se puede definir como una plataforma informática que permite la creación de aplicaciones web (CRM, ERP, entre otros) y sin la complejidad de comprar y mantener el software y la infraestructura debajo de él.

IaaS: Es una forma de ofrecer infraestructura servidores, almacenamiento, red y sistemas operativos, en lugar de comprar servidores, software, espacio de centro de datos o equipos de red, los clientes en su lugar compran esos recursos como un servicio totalmente subcontratado bajo demanda.[7]

---

[5] Varios. (2016). Computación en la nube. 2017, de Wikipedia Sitio web: https://es.wikipedia.org/wiki/Computaci%C3%B3n_en_la_nube

[6] Andreas Maier. (2016). A brief history of cloud computing. 2017, de XXL CLOUD Sitio web: https://xxlcloud.com/en/blog/a-brief-history-of-cloud-computing

[7] Rackspace Hosting. (2011). The Cloud Computing Stack. UNDERSTANDING The Cloud Computing Stack SaaS, Paas, IaaS (17). US

En lo que respecta en administración de datos, la mayoría de las aplicaciones empresariales se basan en una base de datos relacional para el almacenamiento de datos. Al desplegar bases de datos relacionales en la nube, puede elegir entre una gama de opciones que abarcan distintos tipos de servicios y productos. En general, se proporciona dos tipos básicos de servicios de datos relacionales, y cada uno puede admitir diferentes tipos similares a la nube en general:

Plataforma como servicio (PaaS): Este servicio, también puede ser considerado como una base de datos y denominado (DBaaS), dicho tipo de nube elimina la necesidad de administrar el sistema operativo subyacente y la plataforma del servidor de bases de datos. Se centra sólo en tareas específicas de la base de datos.

Infraestructura como Servicio (IaaS): Puede crear máquinas virtuales que alojen una instancia de un sistema de gestión de base de datos relacional (RDBMS), tales como SQL Server, MySQL, entre otras. También puede utilizar cualquier servidor de base de datos compatible con cualquiera de las plataformas del sistema operativo que pueda implementar en las máquinas virtuales, como Oracle, DB2 o SAP HANA.

Finalmente, esta idea de implementación, hizo posible el inicio de una nueva etapa de posibilidades de negocio donde varias empresas formaron parte de esto como: Microsoft (Microsoft Azure), IBM (IBM SmartCloud), Google, entre otras. [8]

Actualmente los distintos proveedores ya no solo ofrecen las tres alternativas antes mencionadas debido a que los usuarios aumentan sus necesidades como, por ejemplo: almacenamiento de información en bases de datos No SQL, aprendizaje automático, IoT, marketing digital, blockchain (plataforma rápida, de bajo costo y bajo riesgo para experimentar con nuevos procesos empresariales), entre otros.

1.2.1 Concepto Cloud Computing

Existen muchas definiciones acerca del Cloud Computing, pero el que más se acerca a mi forma de verlo es: “Una plataforma de Cloud Computing permite que las aplicaciones o datos se alojen en un entorno virtual accesible a Internet que suministra las capacidades necesarias de hardware, software, red y almacenamiento, y proporciona seguridad y fiabilidad, eliminando gran parte de la carga de compra y mantenimiento de hardware y software”.

[8] Información otorgada por Microsoft Ecuador, archivo La nube para los negocios modernos.

En la nube se puede desarrollar, implementar y administrar aplicaciones o datos como lo ha hecho en el pasado e integrar estos servicios a sus aplicaciones locales.

Se paga solamente por el tiempo, los recursos y la capacidad que se utiliza mientras se amplía para adaptarse a las necesidades cambiantes del negocio.[9]

A un nivel general es un estilo de computación donde las capacidades relacionadas con IT son escalables y flexibles al momento que se proporcionan como servicio a clientes externos, además ayuda a las empresas a mejorar la creación y entrega de soluciones IT, accediendo a servicios con menor costo.[10]

La computación en nube ya ha demostrado ser merecedora de atención tanto de las empresas establecidas como de las nuevas empresas. La mayoría de las empresas están considerando la computación en la nube con algo más que una simple curiosidad. Hasta la fecha, las investigaciones de mercado de TI sugieren que la mayoría de los administradores de TI de la empresa tienen recursos suficientes para adoptar el Cloud Computing en combinación con las capacidades de TI locales.

A continuación se tiene otras definiciones que pueden ayudar a entender mejor sobre la nube, según NIST (National Institute of Standards and Technology), "Cloud Computing es un modelo tecnológico que permite el acceso ubicuo, adaptado y bajo demanda en red a un conjunto de recursos compartidos (por ejemplo redes, servidores, equipos de almacenamiento, aplicaciones y servicios) que puede ser rápidamente aprovisionados y liberados con un esfuerzo de gestión reducido o interacción mínima con el proveedor del servicio."[11]

Otra definición muy importante es la ofrecida por Microsoft, "La computación en nube es un cambio en la computación tradicional que ofrece a las empresas el acceso bajo demanda a una variedad de software y servicios de TI, mientras que da un conjunto compartido de recursos informáticos configurables en las capas de la plataforma, de infraestructura y aplicaciones", su objetivo principal es "remover los límites de tu negocio".[12]

[9] Joshy Joseph. (2009). Cloud Computing - Patterns For High Availability, Scalability, And Computing Power With Microsoft Azure. 2017, de MSDN Sitio web: https://msdn.microsoft.com/en-us/magazine/dd727504.aspx
[10] David W. Cearley. (2010). Cloud Computing, Key Initiative Overview, Gartner.
[11] ONTSI (Observatorio Nacional de las Telecomunicaciones y de la SI). (2012). Cloud Computing, Retos y Oportunidades. España: Gobierno de España.
[12] Microsoft. (2016). What is cloud computing? 2017, de Microsoft Sitio web: https://azure.microsoft.com/en-us/overview/what-is-cloud-computing/

Cuando se hace bien, la computación en nube permite a las empresas rapidez, aprovechando el poder de los centros de datos masivos y servicios de TI sin tener que construir, administrar o mantener.[13]

A finales de 2013, International Data Corporation (IDC) publicó un pronóstico que prevé que el gasto mundial en los servicios de Cloud Computing llegaría a 47,400 millones de dólares. Para 2017, pronosticó que este número excedería los 107,000 millones de dólares.[14]

1.2.2 Proveedores extranjeros

En la actualidad existen algunas empresas encargadas en ofrecer servicios de Cloud Computing, y en el año 2015 según la IDG se obtuvo 16% de crecimiento de la demanda de aplicaciones empresariales en la nube a nivel mundial, a continuación, presentaré:

1) **Amazon Web Services:** Ubicada en Seattle, WA, USA. Es un conjunto de servicios de Cloud Computing que conforman la plataforma de computación bajo demanda que ofrece Amazon.com.

   Estos servicios operan desde 12 regiones geográficas en todo el mundo. El más céntrico y bien conocido de estos servicios podría decirse que incluyen Amazon Elastic Compute Cloud, también conocido como "EC2", y Amazon como simple servicio de almacenamiento, también conocido como "S3".

   Amazon AWS comercializa como un servicio para proporcionar gran capacidad informática más rápida y más barata que una empresa cliente la construcción de una granja de servidores físicos reales.

2) **Google Cloud**: Es la versión de Google para ofrecer soluciones empresariales en la Nube. Este proveedor de Cloud permite construir aplicaciones y sitios web, almacenar y analizar datos sobre la infraestructura de Google.

3) **Rackspace:** Ubicada en San Antonio, TX, USA. Es líder en hosting gestionado, con especialistas en virtualización, seguridad, contenedores, datos, comercio electrónico, gestión de contenidos web, correo electrónico y colaboración, recuperación de desastres y transformación de TI.

[13] Microsoft. (2016). What is cloud computing? 2016, de Microsoft Sitio web: https://www.microsoft.com/en-us/server-cloud/solutions/cloud-computing.aspx
14 IDC (2013), "IDC Forecasts Worldwide Public IT Cloud Services Spending to Reach Nearly $108 Billion by 2017 as Focus Shifts from Savings to Innovation", http://www.idc.com/getdoc.jsp?containerId=prUS24298013.

Además, cuenta con hosting dedicado, nube pública y privada con proveedores como son: Microsoft Azure y Amazon Web Services. [15]

4) **Equinix:** Es la plataforma líder de colocación y la interconexión de la industria, que resuelven problemas críticos en torno a escala y el acceso al cliente que determinan el éxito en el mercado, proveen de los siguientes: Amazon Web Services, Microsoft Azure, Google Cloud Platform, CloudSigma y Marketo.

1.2.3 Proveedores Nacionales

En Ecuador con el tiempo se ha implementado en la mayor cantidad de proveedores de servicios en la nube.

Entre el año 2005 y 2010 en el país se tenía pocas empresas que brindaban el servicio de Datacenter.

Así, a partir del año 2010, Telconet inició la construcción de 2 centros de datos certificados por entidades internacionales como el UpTimeInstitute. En ese momento también comenzó a realizar una difusión de lo que existe a nivel internacional en lo que respecta a Centro de Datos y Cloud Computing

A continuación, se presenta diversos proveedores en Ecuador:

1) **HP Ecuador:** Es una empresa estadounidense, de las mayores empresas de tecnologías de la información del mundo, con sede en Palo Alto, California.

Hoy en día esta prestigiosa empresa ofrece Cloud Computing al Ecuador con una amplia cartera de servicios como:

- **HP Helion Managed Cloud Services:** Es infraestructura para cargas de trabajo de aplicaciones críticas que requieren niveles más altos de seguridad, rendimiento, disponibilidad, continuidad, capacidad de respuesta y calidad.

- **HP Helion Managed Cloud – Applications**: Son aplicaciones integradas a través de SAP, Microsoft, Oracle, y software como servicio.

- **HPE Helion Managed Cloud Broker:** Es una visión única de sus gastos de TI, el rendimiento del servicio, configuraciones operativas y postura de seguridad.

[15] Rackspace. (2016). Dedicated Hosting Solutions 2016, de Rackspace Sitio web: https://www.rackspace.com/managed-hosting

- **HP Helion Mobile Enterprise Services:** Ofrecer soluciones innovadoras que mejoran la movilidad manera se involucra a sus clientes e impulsar mejoras en la productividad de sus empleados con los servicios de movilidad.

- **HP Cloud Backup Service Ready Solution**

- **HP Helion and Veritas Continuity:** Servicios de continuidad proporcionan una sólida protección de los entornos complejos de TI.[16]

2) **LOL Cloud:** La Nube de Licencias OnLine.

   Licencias OnLine cuenta con un equipo de trabajo enfocado al Cloud Computing. LOL Cloud cuenta con las herramientas necesarias para aprovechar al máximo este nuevo y rentable negocio.

   Proporciona el soporte, capacitación y los mejores proveedores de servicios del mercado para ayudarlo a crear nubes para sus clientes.

   Con LOL Cloud es más fácil cerrar oportunidades en la nube. Nuestra presencia regional y liderazgo en soluciones de Cloud Computing posicionan como visionarios en esta industria.[17]

3) **Itelsys:** Ofrece servicios IBMConnectionsCloud en Ecuador y es una opción de nube abierta se basan en tecnologías abiertas para garantizar la interoperabilidad y la flexibilidad, así como para ahorrarle tiempo valioso y gastos de desarrollo[18]. Ofrece distintos servicios como:

- Aplicaciones de negocios (SaaS)
- Servicios para desarrolladores (PaaS) – Bluemix
- Servicios de infraestructura (IaaS)
- Nube Privada/Híbrida
- Seguridad
- Cloud Abierto

[16] HP Ecuador. (2016). Servicios Cloud Computing, HP Ecuador. 2016, de HP Sitio web: https://www.hpe.com/lamerica/es/services.html
[17] LOL Cloud. (2016). Información de Costos de Nube. 2016, de Licencia Online Sitio web: http://www.licenciasonline.com/ec/es/cloudhttps://www.hpe.com/lamerica/es/services.html
[18] Información ofrecida por Itelsys

4) **Claro Cloud:** Es un servicio que ya se ofrece en varios países de Latinoamérica, y ahora está presente en Ecuador, con una robusta red de servidores de datos y la mejor tecnología.

   Podrá subir información y acceder a ella a través de smartphones, tabletas o computadoras, desde cualquier lugar. También podrá crear usuarios y tener la disponibilidad de gestionar operaciones y contratar nuevos servicios de forma rápida y accesible.

   Dentro del portafolio que Claro Cloud ofrece se incluyen servicios como servidores y centros de datos virtuales, servicios de seguridad y respaldo de datos, cuentas de correos personalizados, conferencias remotas de audio y video, herramientas de Office 365, así como creación de páginas web, entre otros.[19]

5) **Nexsys Cloud:** Pretende facilitar la compra de servicios tecnológicos sin importar el tipo de tecnología que ofrece el proveedor, los usuarios siempre podrán contar con servicios tecnológicos para la empresa o negocio pagando el uso real y ahorrando costos ya que no tendrá que pagar por software, hardware, el espacio para poder almacenar los equipos y el recurso humano para el mantenimiento, manejo e integración de los componentes para acceder a los servicios tecnológicos que su empresa necesita.

   Son proveedores de: Microsoft, Oracle, HP, entre otros.[20]

6) **Business IT**: Ofrecen servicios de Cloud Computing y migraciones; y cuentan con un servicio adicional llamado Cloud Assessment cubre los posibles riesgos críticos de la transición y sus implicaciones en el área de negocio incluyendo organización, tecnología, seguridad, privacidad, aspectos legales, y otros.

7) **Business Mind**: Recientemente se encuentra implementando el área de la nube para Oracle y servicios en ella con RightNow. Como también Certificación Cloud Computing, Big Data e Inteligencia de Negocios.[21]

8) **Nube Digital:** Infraestructura, soluciones tecnológicas, mesa de servicio local, costo dependiendo su uso.[22]

   Ofreciendo los siguiendo servicios:

   - Correo electrónico
   - Comunicaciones unificadas
   - Almacenamiento
   - Escritorios virtuales

[19] Claro Ecuador. (2016). Servicios Cloud. 2016, de Claro EC Sitio web: www.clarocloud.com.ec/
[20] Información entregada por la empresa
[21] Información obtenida de la empresa
[22] Computerworld. (2015). Cloud. Computerworld, 268

- Mesa de servicios
- Facturación electrónica
- Backup

1.2.4 Comparativo de servicios de proveedores nacionales y extranjeros

Análisis Comparativo de Servicios en la Nube en los distintos proveedores nacionales								
Servicios	HP Ecuador	LOL Cloud (Rackspace, Microsoft Azure, Citrix)	Itelsys (IBM Connection, Office 365)	Claro Cloud (Office 365)	Nexsys Cloud	Business IT (Enterprise Mobility Suite)	Business Mind (Oracle Cloud)	Nube Digital
Servicios de Aplicaciones	Sí	Sí	No	No	Sí	Sí	Sí	No
Múltiples Ambientes	Sí	Sí	No	No	Sí	No	Sí	No
Almacenamiento	Sí	Sí	Sí	Sí	Sí	No	Sí	No
Bases de Datos SQL	Sí	Sí	No	No	No	No	Sí	No
Máquinas Virtuales	Sí	Sí	No	Sí	No	No	Sí	No
Servicios en la nube	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí
Active Directory	No	Sí	No	No	No	Sí	No	No
Bases de Datos NoSQL	No	Sí	No	No	No	No	Sí	No
Backup	Sí	Sí	No	No	No	Sí	Sí	No
Correo Nube	No	Sí	Sí	Sí	No	No	Sí	Sí
Remote App	No	Sí	No	No	No	No	Sí	Sí
Infraestructura Virtual	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí

Tabla 1: Cuadro comparativo de proveedores nacionales

Fuente: (Lozada, 2016)

Análisis Comparativo de Servicios en la Nube en los distintos proveedores extranjeros				
Servicios	Amazon (AWS)	Google Cloud	Rackspace (Microsoft Azure, AWS)	Equinix (CloudSígma, Microsoft Azure, AWS, Google Cloud
Servicios de Aplicaciones	Sí	Sí	Sí	Sí
Múltiples Ambientes	Sí	Sí	Sí	Sí
Almacenamiento	Sí	Sí	Sí	Sí
Bases de Datos SQL	Sí	Sí	Sí	Sí
Máquinas Virtuales	Sí	Sí	Sí	Sí
Servicios en la nube	Sí	Sí	Sí	Sí
Active Directory (Microsoft Azure)	No	No	Sí	Sí
Bases de Datos NoSQL	Sí	Sí	Sí	Sí
Backup	Sí	Sí	Sí	Sí
Correo Nube	No	Sí	Sí	Sí
Remote App	Sí	Sí	Sí	Sí
Infraestructura Virtual	Sí	Sí	Sí	Sí
Tienda	Sí	Sí	Sí	Sí

Tabla 2: Cuadro Comparativo de Proveedores Extranjeros

Fuente: (Lozada, 2016)

Según los distintos servicios que ofrece cada uno de los proveedores nacionales, en sí todos son muy buenos dependiendo de cuál sea el objetivo final de la empresa o cliente; pero el que ofrece una amplia cartera de servicios es LOL Cloud, empresa que ofrece Microsoft Azure, Rackspace, Symantec Cloud (copias de seguridad y recuperación de datos), Citrix, VMWare, Zimbra (correos), Plataforma completa de Microsoft.

En el caso de proveedores extranjeros, el análisis de servicios por proveedor se obtuvo igualdad entre dos proveedores, Rackspace y Equinix.

Comenzando por Rackspace aparte de ofrecer los beneficios de su nube como Datacenters, Hosting Dedicados entre otros, ofrece Microsoft Azure y Amazon Web Services de los cuales estos dos últimos son nubes muy completas. En el caso de Equinix encontramos Cloud Sigma una nube que se la puede implementar en Suiza y Estados Unidos destacada en servicios de Infraestructura (IaaS), Microsoft Azure, Amazon Web Services de los cuales ya he hablado anteriormente, y Google Cloud, la nube de google la cual tiene ventajas de forma gratuita como también de manera pagada.

1.2.5 Nivel de Adopción Cloud Computing

Cloud Computing hoy en día es una de las opciones con mayor posicionamiento convenientes, generando rentabilidad a sus proveedores, aunque puede presentarse riesgos, al enfocarse en trabajar con esta tecnología, permite economizar el costo tanto en licencias, servidores, almacenamiento, administración de servicios, entre otros.

Para empresas y usuarios individuales, el grado de adopción del Cloud Computing se encuentra directamente relacionado con el nivel del conocimiento sobre este nuevo modelo de operación. El objetivo principal para que la adopción de los servicios Cloud Computing es primeramente proporcionar a las empresas y usuarios un mayor conocimiento y confianza en sus funcionalidades.

La optimización de costos no es el único factor que impulsa a las empresas y usuarios individuales a implementarlo o utilizarlo como su modelo de operación, caso contrario la necesidad de acceder a los datos y servicios desde cualquier lugar es el principal factor que da como resultado a la adopción de Cloud Computing. Así como también la mitigación de riesgos y la innovación son factores muy importantes para todo tipo de usuario o empresa.

Según la encuesta **CloudView**, realizada por IDC y solicitada por CISCO en el año 2016, indica que los participantes contaron con un aproximado de 11.000 encuestados correspondientes a 31 países; de los cuales más de 6.000 con vasta experiencia en la nube que los califica para responder una amplia gama de preguntas en torno al Cloud Computing.

Los temas que se incluyeron fueron: la adopción de las cargas de trabajo específicos de nubes, madurez, criterios de transformación, toma de decisiones en gastos y espera que los beneficios del distinto tipo de nube: híbrida, pública y privada.

Los datos presentados en la encuesta realizada por IDC ponen en comparación como los niveles de adopción de la nube han cambiado desde 2015 hasta 2016[23], en base a la siguiente pregunta:

¿Cómo describir mejor los planes actuales o corto plazo de su organización para utilizar la nube pública o soluciones de nube privada para soportar las cargas de trabajo de producción y servicios?

Perfil de los participantes en la encuesta:

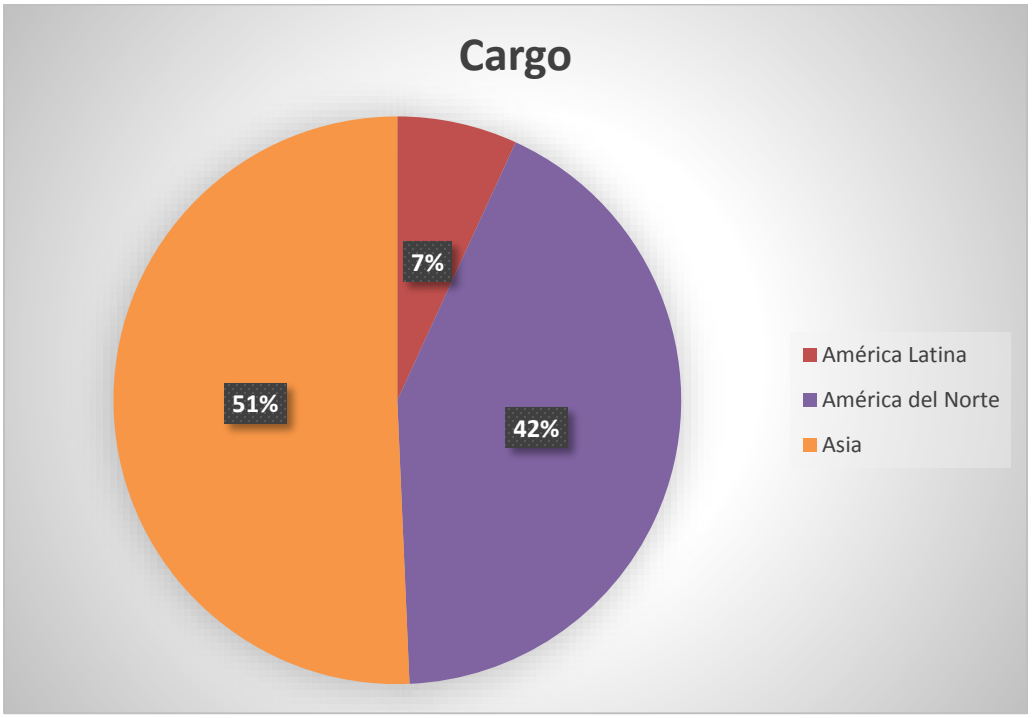


Ilustración 1: Perfil de encuestados de CloudView 2016; por cargo

Fuente: (IDC, 2016)

23 IDC. (2016). CloudView 2016: The Rapid Embracement of Cloud. 2016, de IDC Sitio web: http://www.idc.com/getdoc.jsp?containerId=US41636616

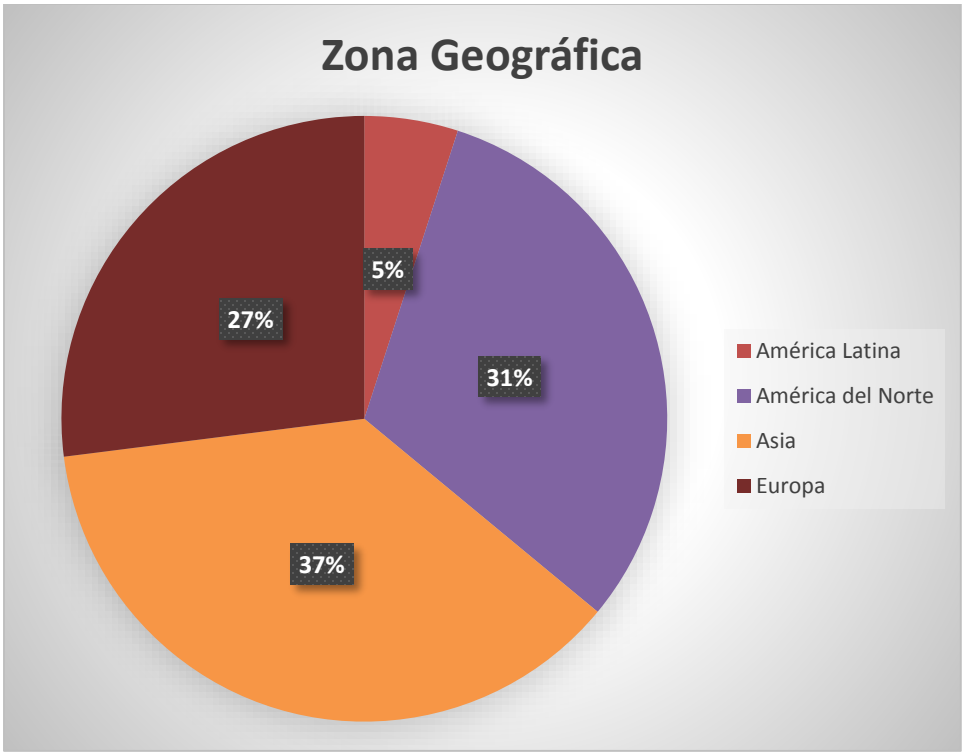


Ilustración 2: Perfil de encuestados de CloudView 2016; por zona geográfica

Fuente: (IDC, 2016)

Resultados del estudio:

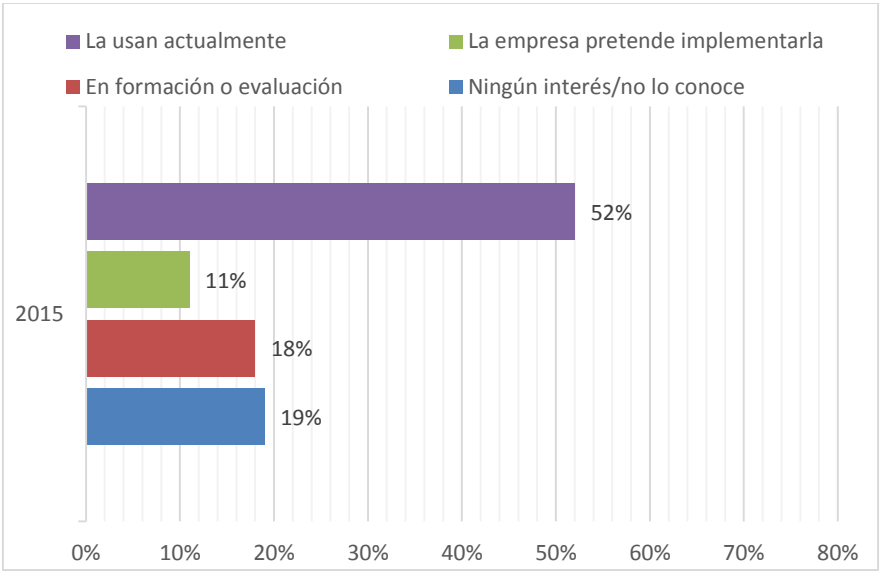


Ilustración 3: Análisis de adopción de nube en CloudView 2016

Fuente: (IDC, 2016)

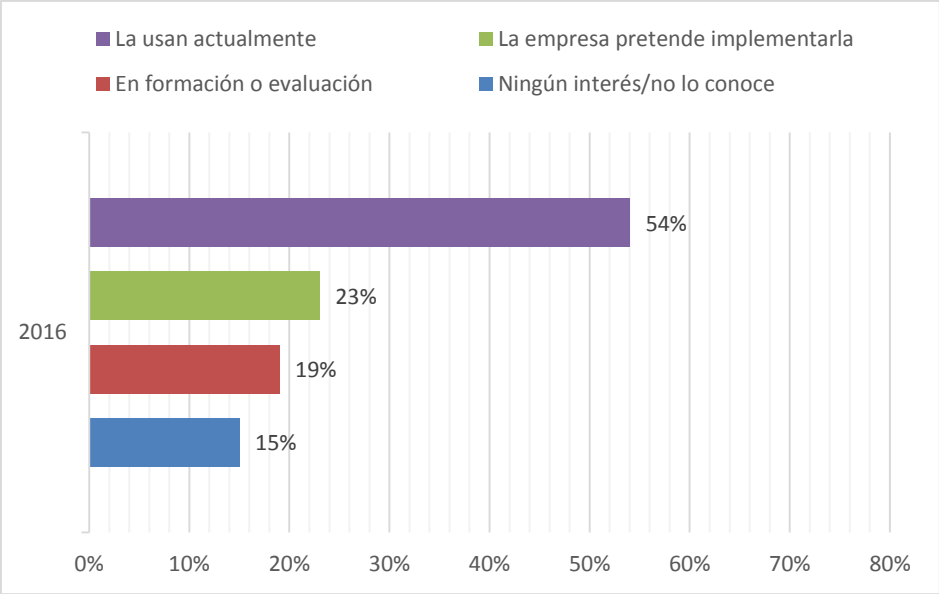


Ilustración 4: Análisis de adopción de nube en CloudView 2016

Fuente: (IDC, 2016)

Casi el 68% de las organizaciones utiliza algún tipo de nube, lo que representa un aumento del 26% con respecto al año pasado.

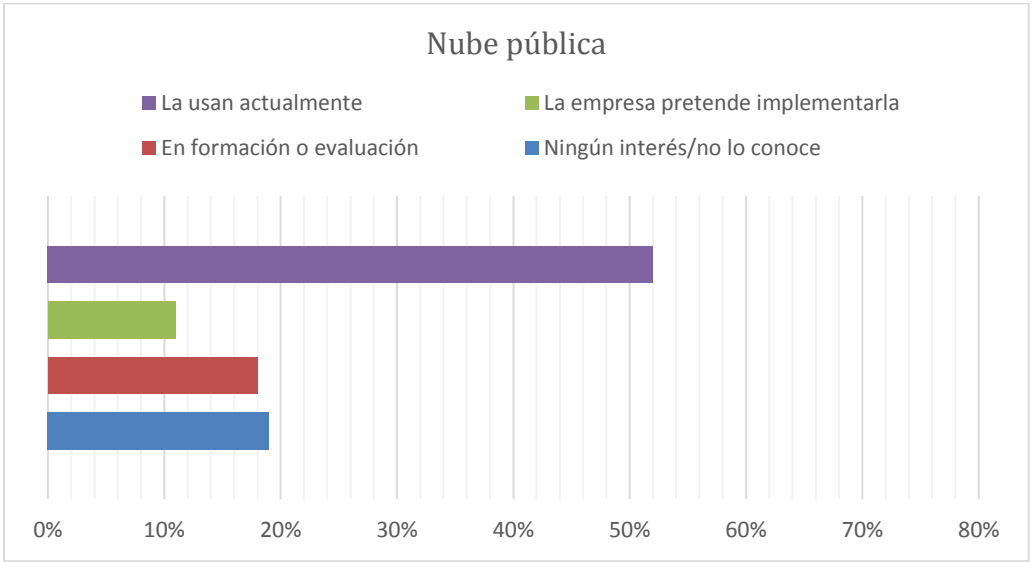


Ilustración 5: Análisis de adopción de nube pública en CloudView 2016

Fuente: (IDC, 2016)

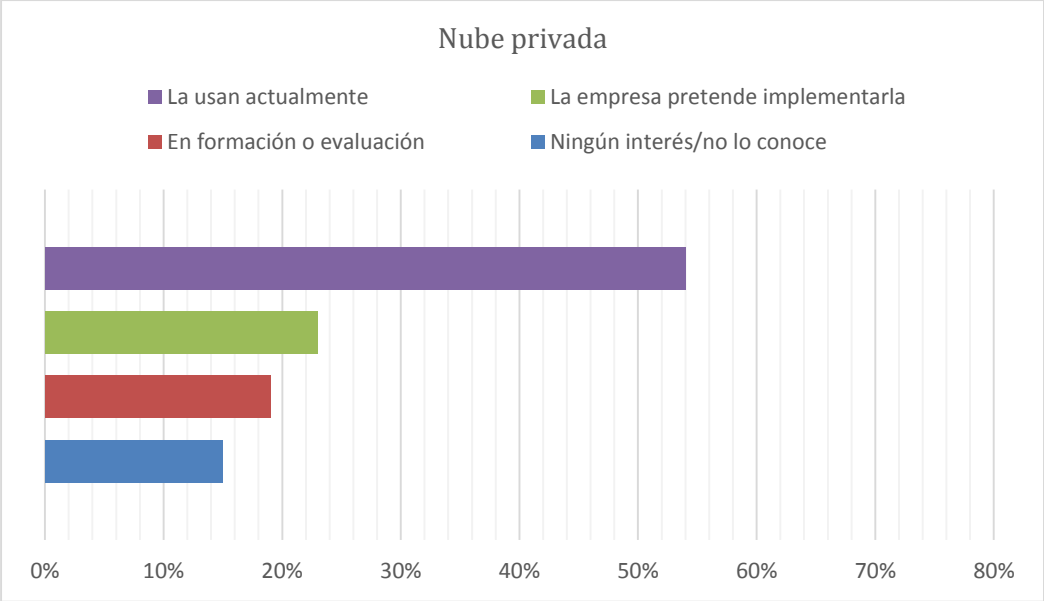


Ilustración 6: Análisis de adopción de nube privada en CloudView 2016

Fuente: (IDC, 2016)

Las organizaciones esperan aumentar su implementación en la nube privada en un 31%, mientras que en la nube pública en un 29% durante los próximos años. La mayoría de personas que adoptan la nube utilizan en un 73% una estrategia de nube híbrida.

Mientras tanto según Frost & Sullivan (empresa de consultoría de negocios involucrados en la investigación y análisis de mercado, estrategia de crecimiento y entrenamiento empresarial a través de múltiples industrias) en el año 2009 ha identificado 5 principios básicos para la adopción de colaboración en la nube y varias oportunidades; amenazas en cada uno de estos dos sectores de industria.

1. **Es clave que la alta gerencia tenga claro los beneficios y los conceptos:** Debe existir despliegue de arriba hacia abajo en la infraestructura organizacional. El despliegue se propone de arriba hacia abajo ya que la nube es quien debe adaptarse a las necesidades de la compañía y no la compañía a los servicios prestados por la nube; contrario de la adopción, es posible que la empresa sufra un proceso de enseñanza para aprender a utilizar los servicios disponibles en la nube generando en su mayor parte molestias a los usuarios finales.

2. **Tener claro las políticas y estándares:** Todos los procesos o componentes de cada proceso basado en la nube deben estar estandarizados y definidos con políticas claras y donde toda la organización este alineada.

3. **Toda introducción de una novedad, genera capacitaciones,** informativos, gerentes de proyecto y mayor organización para alinear la empresa bajo un solo concepto

4. **No re-inventar la rueda.** Identificar compañías que hayan tenido un despliegue de aplicaciones en la nube y proponer mejoras aplicadas al negocio. Usar herramientas de baja inversión como el ciclo de vida del software (análisis, diseño, implementación y pruebas) aplicados a la disposición de aplicaciones corriendo sobre la nube, analice su infraestructura actual vs. el ambiente escalable que le proporciona la nube. ¿Realmente lo necesita?

5. **En caso de no estar seguro de los beneficios de la nube en su compañía,** inicie disponiendo procesos no críticos en la nube y analice periódicamente los beneficios que ha obtenido a cambio en periodos regulares de tiempo.[24]

1.2.6 Beneficios Cloud Computing

Hoy en día la nube se está convirtiendo en una parte importante de las estrategias de mejora en las empresas de TI, o en empresas con gran cantidad de datos las cuales pueden ser: farmacéuticas, petroleras, retail, etc.

Aunque la nube no tiene la respuesta a todas las necesidades de TI o empresariales, tiene grandes beneficios.

Las principales ventajas son:

1. **Flexibilidad**, con este término se refiere a que se puede adquirir varios servicios, aplicaciones, pero cuando se necesita ampliar nuestra empresa se puede comprar y adaptarse, así como cuando ya no se desee alguno de estos.

2. **Actualizaciones de software automáticas**.

3. **Reducción de Costos** en el área de tecnologías y demás involucradas, tú pagas lo que consumes, los costos disminuyen debido a que no tienes que adquirir hardware avanzado y a gran costo, como tampoco someterse a la compra de licencias costosas.

4. **Disponibilidad**, los recursos están disponibles en cualquier lugar, a cualquier hora o donde se requiera, administrado por medio de niveles de seguridad.

[24] Frost & Sullivan. (2015). 5 principios de Adopción en la Nube. 2016, de Coursehero Sitio web: https://www.coursehero.com/file/pglmvu/Frost-Sullivan-ha-identificado-5-principios-b%C3%A1sicos-para-la-adopci%C3%B3n-de/

5. **Escalabilidad**, se accede a la mayor cantidad de servicios según sea las necesidades de la empresa, ya sea por almacenamiento o cualquier otro requerimiento, siempre es recomendable realizar un estudio de negocio previo antes de obtener nuevos servicios.

6. **Fiabilidad**, antes la información se perdía debido a daños en servidores o equipos, al manejar su información en la nube, hoy en día por medio de la redundancia permite a las empresas tener continuidad y capacidad de recuperación de datos ante cualquier desastre.

7. **Multiusuario**, los costos y recursos se reparten en una gran cantidad de usuarios, permitiendo a varios usuarios acceder a una misma aplicación o información a la vez.

1.2.7 Limitaciones Cloud Computing

Así como existe una gran cantidad de ventajas, también podemos encontrar con algunas limitaciones debido a que todavía la nube es una tecnología en desarrollo, dichas limitaciones hablaremos a continuación:

Alta latencia: Las aplicaciones alojadas en la nube sufren con el problema asociado a la latencia generada por conexiones WAN (Wide Area Network) con la que los usuarios acceden a sus respectivos servicios en la nube, esta restricción hace que las aplicaciones con tareas de gran procesamiento no sean óptimas para usar este modelo, mientras que la aplicación con transferencia de gran volumen de datos en tiempo real no sea posible o poco eficaz.

Conexiones de red: El cliente al momento que concibe con servicios debe contar con una conexión de red fiable y estable.

Si hay problemas de conectividad, el acceso a la nube también se convierte en un problema. El rendimiento de las aplicaciones en la nube también depende de la actuación de la red en el lado de los clientes.

Velocidades de carga y descarga son más lentos en comparación con la de un servidor local.

Control de la seguridad de la información: El cliente no tiene el control sobre la seguridad de sus propios datos o no cuenta con un sistema de seguridad implementando tales como normas, estándares, metodologías y herramientas; permitiendo que los datos o activos de información se encuentren susceptibles a la piratería, cibercrimen, ataques de phishing o robo total o parcial de sus datos.

Dado que los servidores en la nube están interconectados, es vulnerable a que cualquier tipo de malware se propague.

Costos adicionales: A pesar que la nube es conocida por el beneficio de ahorro en costos, mantiene algunos costos adicionales no incluidos al momento de la adquisición, por ejemplo, mantenimientos (preventivos, programado, requeridos), actualizaciones, escalabilidad o un plan de seguridad continúa personalizado según los requerimientos de cada usuario o empresa.

Periféricos: Los dispositivos periféricos como impresora o escáneres podrían no funcionar con la nube. Mucho de ellos requieren que se instale software local.

Integración: Las aplicaciones internas, bases de datos, software e infraestructura al momento de acoplarse con la nube resultará complejo y en algunos casos no viables o no compatibles.[25]

1.3 Principales metodologías de seguridad en la nube

La seguridad informática hoy en día es un punto importante y es una de las mayores preocupaciones de las empresas o individuos. Poco a poco se ha popularizado los servicios de almacenamiento en la nube y las estadísticas de crimen cibernético se incrementó según el reporte de Norton año 2016, 689.4 millones equivalente al 31% ha lidiado con algún tipo de crimen informático a nivel mundial[26], por eso la gran parte de empresas han tratado de estudiar amenazas y vulnerabilidades e implementar metodologías de seguridad algunas de ellas detalladas a continuación:

1. **ISO/IEC 27018:** Es la primera norma internacional acerca de la seguridad de datos personales en la nube, dicha norma ya se encuentra más de un año y medio disponible y es una forma de proporcionar confianza, seguridad y privacidad a los usuarios de la nube por medio de su proveedor de servicios.

   La norma ISO/IEC 27018 específica ciertos tipos de medidas de seguridad mínimos que deben adoptar los proveedores de nube al implementar políticas de sensibilización sobre seguridad y hacer que el personal pertinente esté al tanto de las potenciales consecuencias para el proveedor, clientes o personal.

[25] Uma Avantsa. (2011). Limitations of Cloud Computing. 2016, de Meghainfotech Sitio web: https://meghainfotech.wordpress.com/2011/04/21/limitations-of-cloud-computing/

[26] Symantec. (2016). Informe Norton sobre Ciberseguridad 2016, 2016, de Norton Sitio web: https://www.symantec.com/content/dam/symantec/mx/docs/reports/2016-norton-cyber-security-insights-comparisons-mexico-es.pdf

Los objetivos principales de la norma son los siguientes:

- Ayuda a los proveedores de servicios en la nube que procesan datos personales hacer frente a las obligaciones legales aplicables, así como a las expectativas del cliente.

- Habilita la transparencia para que los clientes puedan elegir servicios en la nube bien gobernados.

- Facilita la creación de contratos de servicios (SLAs) en la nube.

- Proporciona a los clientes en la nube un mecanismo para garantizar que los proveedores de la nube cumplan con las obligaciones legales y otras.

Al seguir las normas de ISO/IEC 27001 y el código de conducta integrado con ISO/IEC 27018, la nube demuestra que sus directivas y procedimientos de privacidad son sólidos, de conformidad con estas estrictas normas. [27]

A continuación, se detalla puntos importantes al momento de optar por dicha norma:

5 cosas importantes que se debe conocer de la ISO/IEC 27018

1. La nueva norma se basa en las normas de seguridad de la información existentes incluyendo ISO/IEC 27001 e ISO/IEC 27002.

2. La combinación de un conjunto común de objetivos de control, controles y directrices basados en ISO/IEC 27002, y los objetivos específicos de control adicionales en la nube y otros controles, ayudar a gobernar el tratamiento de los datos personales en la nube.

3. Los proveedores de la nube pueden cumplir con las obligaciones aplicables.

4. La transparencia permite a los clientes de los servicios en nube seleccionar servicios de procesamiento de datos personales bien gobernados en la nube.

5. El mecanismo para el ejercicio de los derechos de auditoría y cumplimiento ayudar a prevenir riesgos para proteger los datos personales. [28]

[27] Microsoft. (2016). Código de conducta para proteger los datos personales en la nube: ISO/IEC 27018. 2017, de Microsoft Sitio web: https://www.microsoft.com/es-xl/TrustCenter/Compliance/ISO-IEC-27018
[28] Varios. (Febrero 2015). ISO 27018. ISOfocus en el cloud, 52.

2. ISO/IEC 27001:

ISO 27001 es una norma internacional publicada por la Organización Internacional de Normalización (ISO), y describe cómo gestionar la seguridad de la información en una empresa.

La última revisión de esta norma se publicó en 2013 y su título completo es ahora ISO / IEC 27001: 2013.

Se puede implementar en cualquier tipo de organización, lucrativa o sin fines de lucro, privada o de propiedad estatal, pequeña o grande. También permite a las empresas certificarse, lo que significa que un organismo de certificación independiente basado en metodologías y documentación permite a la organización implementar la políticas y estándares de seguridad de la información conforme a la norma ISO/IEC 27001.

ISO/IEC 27001:2013 se ha convertido en este tiempo en el estándar de seguridad de la información más popular en todo el mundo y muchas empresas han obtenido tal certificado.

El enfoque de ISO/IEC 27001 es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa. Esto se logra averiguando qué posibles problemas podría pasar a la información, por medio de distintos análisis tales como la evaluación del riesgo, definición de actividades de mitigación de riesgo, mitigación del riesgo por medio de controles o el tratamiento del riesgo.

Los controles que se implementan son en forma de políticas, procedimientos o herramientas adicionales (por ejemplo, software o hardware). Sin embargo, en la mayoría de los casos las compañías ya tienen todo el hardware y software en su lugar, pero lo están usando de una manera poco segura. Por lo tanto, la mayoría de la implementación ISO/IEC 27001 será sobre el establecimiento de reglas de organización necesarias para prevenir las violaciones de la seguridad. Dado que dicha implementación requerirá múltiples políticas, procedimientos, personas, activos, etc., la ISO/IEC 27001 ha descrito cómo integrar todos estos elementos en el sistema de gestión de la seguridad de la información (SGSI).[29]

Actualmente, la infraestructura y los servicios de nube de Microsoft son auditados una vez al año por la norma ISO / IEC 27001 cumplimiento todos los requerimientos por el British Standards Institution (BSI), un organismo de certificación acreditado, que proporciona una

[29] Dejan Kosutic. (2016). ISO 27001:2013 FOUNDATIONS COURSE. 2016, de Advisera Sitio web: https://training.advisera.com/course/iso-27001-foundations-course/

validación independiente que Microsoft ha implementado controles de seguridad de extremo a extremo. [30]

3. **HIPAA:** Health Insurance Portability and Accountability Act, establece el estándar para proteger los datos o información sensible de los pacientes. Cualquier empresa que se ocupa de información confidencial de salud debe asegurar que todos los requerimientos físicos, red, y de procesos mantenga la seguridad requerida. Esto incluye entidades cubiertas, cualquier persona que ofrece tratamiento, operaciones en cuidado de la salud, socios de negocios, cualquier persona con acceso a la información del paciente y que proporciona apoyo en el tratamiento, pago u operaciones.

   La Regla de Privacidad HIPAA aborda el ahorro, el acceso y el intercambio de información médica y personal de cualquier individuo, mientras que la Regla de Seguridad HIPAA es más específica en las normas nacionales de seguridad para proteger los datos de salud creados, recibidos, almacenados o transmitido electrónicamente, también conocido como protección de información de salud.

   Si usted es anfitrión de sus datos con un proveedor de alojamiento compatible con HIPAA, deben tener ciertas medidas de seguridad administrativas, físicas y técnicas en su lugar, de acuerdo con el Departamento de Salud y Servicios Humanos de EE.UU o de su país. Las medidas de seguridad física y técnicas son más relevantes para los servicios proporcionados por su proveedor de alojamiento HIPAA se enumeran a continuación.

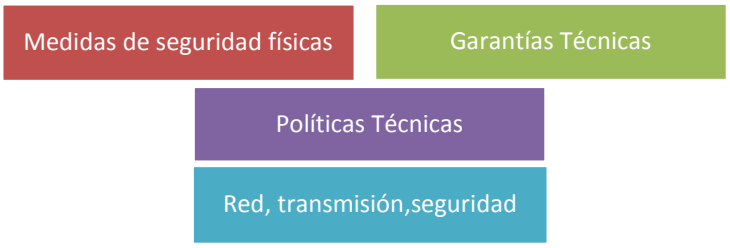


Ilustración 7: Servicios HIPAA

Fuente: (Onlinetech, 2016)

[30] Microsoft Trust Center. (2015). ISO/IEC 27001. Abril, 2016, de Microsoft Sitio web: https://www.microsoft.com/en-us/TrustCenter/Compliance/ISO-IEC-27001

4. **CPS:** La entrega de contenido y la asociación de seguridad (CDSA), es un organismo de normalización mundial para el entretenimiento y software de industria, ellos han entendido desde hace tiempo la necesidad de sus miembros para operar de manera individual y en conjunto con seguridad, particularmente en un panorama en donde las amenazas evolucionan de manera impresionante.

Como resultado, la CDSA desarrolló el **Estándar de Contenido de Protección y Seguridad (CPS)** para proporcionar un conjunto de controles diseñados para asegurar la continuidad de la integridad de la propiedad intelectual, la confidencialidad y seguridad de los activos de medios en todas las etapas de la cadena de valor. [31]

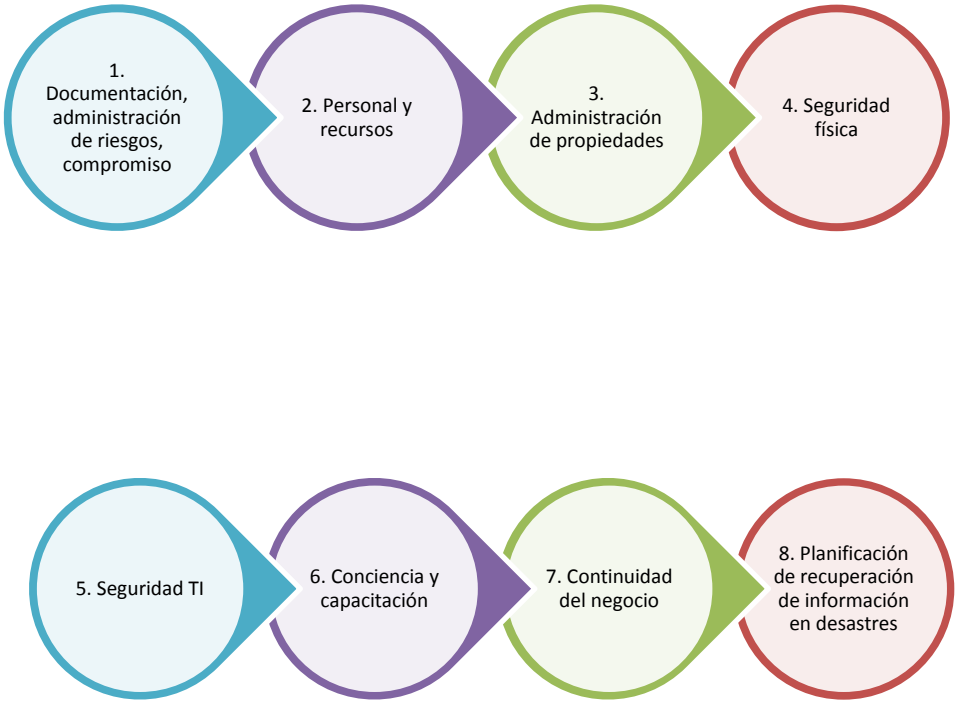


Ilustración 8: Pasos a seguir para implementación de estándar CPS

Fuente: (CDSA, 2013)

[31] CDSA. (2013). Content Delivery & Security Association Anti-Piracy & Compliance Programs CPS Certification Program Overview. Abril 2016, de CDSA Sitio web: http://www.cdsaonline.org/wp-content/uploads/2013/05/CDSA-Content-Protection-Security-Standard-Overview.pdf

5. **Reportes SOC 1, 2 y 3:** Las empresas con el tiempo se encuentra externalizando funciones básicas tales como el almacenamiento de datos y el acceso a las aplicaciones por medio de proveedores de nube (CSPs).

El Instituto Americano de Contadores Públicos Certificados (AICPA) ha desarrollado el marco de referencia denominado Servicio de Control de Organización (SOC), un estándar para los controles que protegen la confidencialidad y privacidad de la información almacenada y procesada en la nube. Esto se alinea con la Norma Internacional sobre Compromisos de Aseguramiento (ISAE), la norma de información para las organizaciones de servicios internacionales.

Servicios de Auditorías basado en el marco SOC se divide en dos categorías: SOC 1 y SOC 2 localizados como alcance en los servicios de la nube de Microsoft.

Microsoft es auditado anualmente con respecto a la estructura de información SOC por medio de auditores independientes contratados por terceros. La auditoría de servicios demostró que la nube de Microsoft cubre los controles de seguridad de los datos, la disponibilidad, la integridad de procesamiento, y la confidencialidad como principios aplicables a la confianza en el ámbito de cada servicio.

Microsoft ha logrado informes SOC 1 Tipo 2, SOC 2 Tipo 2 y SOC 3. En general, la disponibilidad de informes SOC 1 y 2 está restringida a los clientes que han firmado acuerdos de confidencialidad con Microsoft; el informe SOC 3 está disponible públicamente.

	¿Qué se reporta?	¿Quién lo usa?
SOC 1	Controles internos sobre informes financieros.	Usuarios auditores y usuarios contralores de oficina
SOC 2	Seguridad, disponibilidad, integridad de procesamiento, confidencialidad o controles de privacidad.	Gerencia, reguladores y otros. Compartido bajo acuerdo de confidencialidad
SOC 3	Seguridad, disponibilidad, integridad de procesamiento, confidencialidad o controles de privacidad.	Públicamente disponible para todos.

Tabla 3: Cuadro de especificación de funciones y usuarios SOC 1, 2, 3

Fuente: (Pham, 2011)

1.4 Análisis de seguridad de cada una de las metodologías.

El punto anterior se revisó las posibles metodologías, cada una con características especiales según el negocio y necesidades de los usuarios.

Hoy en día proteger la información es muy importante, la cual representa la fuente de valor de la mayoría de empresas en donde su administración y control debe ser permanente durante todas sus etapas: Generación o creación, almacenamiento, transmisión (envió y recepción).

Para poder asegurar la información se conoce que existen distintos certificados, métodos, estándares de los cuales algunos se encuentran dedicados a proteger información específica tales como: **HIPAA** para la protección de información médica; **SOC 1,2,3** para proteger confidencialidad y privacidad de la información contable; **ISO/IEC 27018** para administración de datos personales de los diferentes usuarios alojados en la nube; **ISO/IEC 27001** es uno de los estándares más populares y con gran número de implementaciones en Cloud Computing y **CPS** es una norma utilizada en procesos de auditoria informática.

Las normas o metodologías mencionadas anteriormente ya se encuentran disponibles e implementadas en Microsoft Azure, Rackspace, Google, entre otros proveedores de nube.

En conclusión, es muy importante la implementación de políticas, estándares, metodologías y herramientas; para proteger los centros de información, vías de comunicación e infraestructura crítica contra los ataques maliciosos y las amenazas del ciberespacio en empresas y usuarios individuales.

CUADRO COMPARATIVO DE METODOLOGÍAS DE SEGURIDAD					
	ISO/IEC 27001	**ISO/IEC 27018**	**HIPAA**	**CPS (CDSA)**	**SOC 1,2,3**
Característica Principales	Estándar de seguridad que especifica formalmente un Sistema de Gestión de Seguridad de la Información (SGSI o ISMS) que está destinada a traer seguridad de la información bajo el control explícito de la dirección.	Es la primera norma internacional sobre la seguridad de datos personales en la nube, dicha norma ya se encuentra más de un año y medio disponible y es una forma de proporcionar confianza a los usuarios de la nube de que el proveedor de servicios pueda mantener sus datos seguros y privados.	Health Insurance Portability and Accountability Act, establece el estándar para proteger los datos sensibles de los pacientes. Cualquier empresa que se ocupa de información confidencial de salud debe asegurar que todos los requerimientos físicos, red y procesos mantenga la seguridad requerida.	Estándar de Contenido de Protección y Seguridad (CPS) para proporcionar un conjunto de controles diseñados para asegurar la continuidad de la integridad de la propiedad intelectual, la confidencialidad y seguridad de los activos de medios en todas las etapas de la cadena de suministro	Estándar para los controles que protegen la confidencialidad y privacidad de la información almacenada y procesada en la nube. Esto se alinea con la Norma Internacional sobre Compromisos de Aseguramiento (ISAE), la norma de información para las organizaciones de servicios internacionales.
Implementación en Nube	Sí	Sí	Sí	Sí	Sí
Área de Implementación	Tecnologías de la Información, Banca, Consultoría	Tecnologías de la Información	Aseguradoras, Área de Recursos Humanos, Hospitales	Banca, Tecnología de la información, Universidades	Empresas Auditoras, Banca
Empresas que lo utilizan	Microsoft, Rackspace, Amazon, Google	Microsoft, Amazon, Google	Microsoft, Amazon, Google, Rackspace	Microsoft, Rackspace, Google	Microsoft, Rackspace, Amazon

Tabla 4: Tabla Comparativa de Metodologías de Seguridad en la nube

Fuente: (Lozada, 2016)

1.5 Selección de las dos mejores metodologías para realizar el diseño de esquema de seguridad.

Cada una de las metodologías anteriormente expuestas ofrece un método sistematizado para identificar y analizar vulnerabilidades y riesgos, adicionalmente cada uno lleva una planificación para la correcta selección de controles y medidas necesarias para mitigarlos utilizando herramientas que faciliten su análisis y hallazgo.

Para mitigar los riesgos que pueden afectar nuestra información, se revisó y analizó ciertas normas, estándares, certificados y metodologías, por medio de las cuales se orientará a un objetivo fundamental, seleccionar dos de las cuales se acoplen a nuestros activos de información para dicho estudio. Con un análisis previo y asociando cada una de las definiciones el estándar ISO/IEC 27001 es ideal para las necesidades del negocio, dicha norma fue escogida debido a su gran demanda de implementación en la nube y con un gran número de implementaciones referente a seguridad informática y el estándar ISO/IEC 27018 correspondiente a la segunda metodología seleccionada, es una norma dedicada a la seguridad de datos personales en la nube y comúnmente se complementan al utilizarla en conjunto con la primera seleccionada.

Con las metodologías o estándares escogidos se procederá por medio de una serie de pasos y documentos específicos a cumplir los objetivos del Sistema de Gestión de Seguridad Informática SGSI, el mismo permitirá dar a conocer las debilidades y fortalezas de nuestra empresa que forma parte de estudio para cada uno de sus activos de información seleccionados; se logrará identificar, evaluar y valorar los procesos del negocio con el propósito de conocer si el nivel de protección y controles de seguridad (si aplica) es el adecuado y con un alto nivel de efectividad para poder afrontar la mayor parte de riesgos, vulnerabilidades y amenazas.

A continuación, en la **Ilustración 9** podemos visualizar un modelo preliminar de nuestro Sistema de Gestión de Seguridad de la Información basado en las metodologías seleccionadas e información entregada para el estudio.

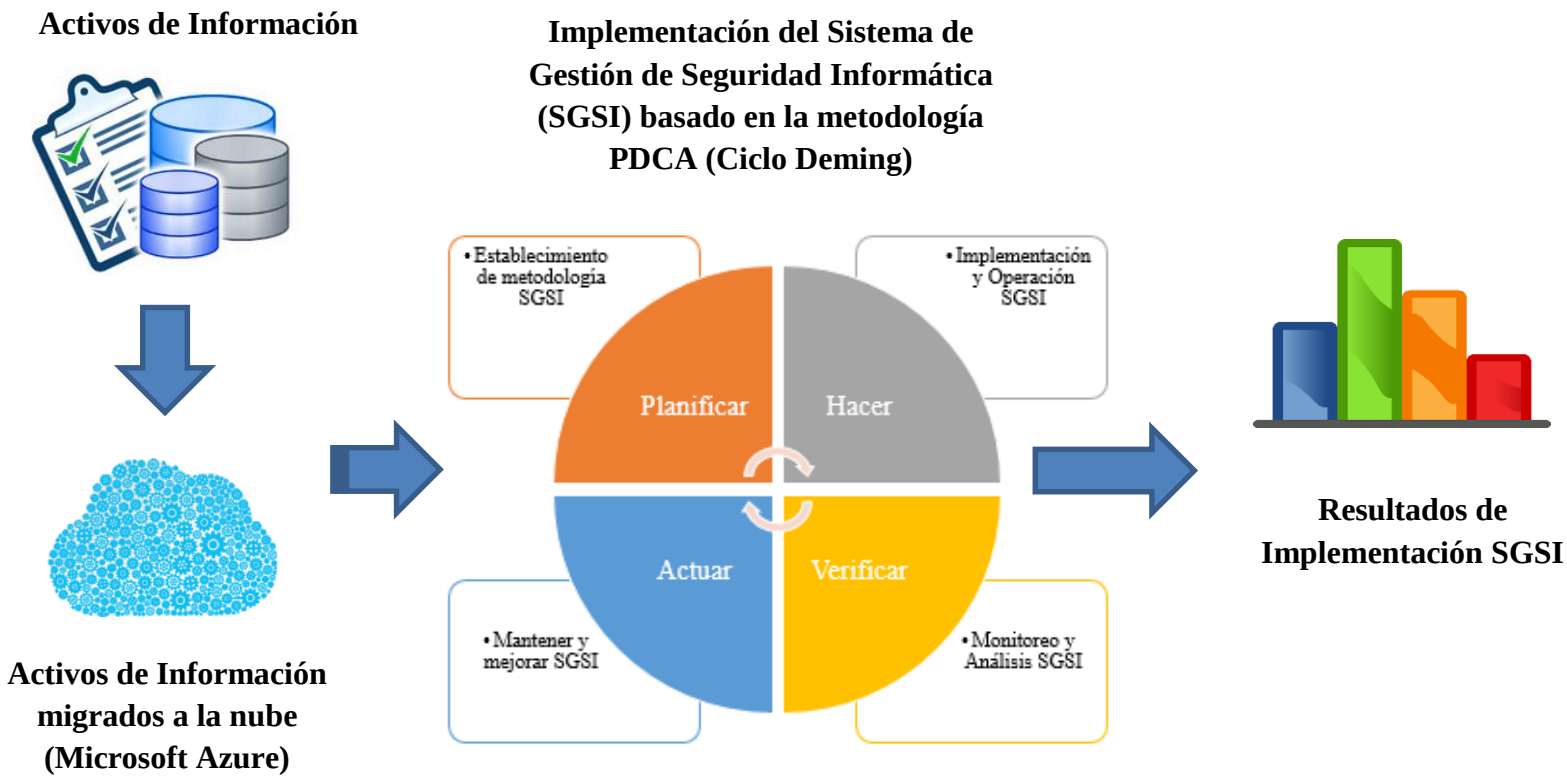


Ilustración 9: Modelo preliminar de diseño de esquema de seguridad

Fuente: (Lozada, 2016)

Capítulo II: Análisis comparativo sobre seguridad

2.1 Preocupaciones al momento de adoptar Cloud Computing

Hoy en día las compañías requieren utilizar soluciones seguras, Cloud Computing es una de ellas, esta solución permite reducir costos, riesgos y recursos de administración con respecto a hardware y software.

Según datos públicos y recogidos por beServices en junio del 2017, consultora especializada en proyectos TIC y proveedores de soluciones informáticas de infraestructura Cloud Computing, el problema de la seguridad y los sistemas de pago continúan siendo el mayor impedimento para la adopción de la nube pública. De hecho, un 64 % de los directores TI no colocan una o más cargas de trabajo en la nube por miedo al acceso no autorizado a sus datos.

Asimismo, al 25% también les preocupa que la decisión de nube no consiga generar suficiente rentabilidad. Y es que la nube pública bajo la fórmula de pago por uso puede suponer un coste total de propiedad más elevado que el de un centro de datos equipado.[32]

A continuación, se detallará las principales preocupaciones que son persistentes por el lado del cliente y empresas tales como seguridad de la información, privacidad y confiabilidad.

2.1.1 Seguridad de la información

Los clientes de distintos proveedores de servicios en la nube quieren estar seguros de que la seguridad diseñada, establecida o implementada que han confiado a su proveedor se cumpla y mantenga al menos un nivel estándar de seguridad.

Para algunas organizaciones, los retos de seguridad en la nube son aún mayores, ya que estos requieren ciertos requisitos legales y regulatorios de cada país como por ejemplo el

[32] Computerworld México. (2017). El 64% De Las Empresas Temen La Adopción De La Nube Pública Por Problemas De Seguridad. 2017, de Computerworld Sitio web: http://computerworldmexico.com.mx/64-las-empresas-temen-la-adopcion-la-nube-publica-problemas-seguridad/

estándar de **Ley de Portabilidad y Responsabilidad del Seguro de Salud (HIPAA)** para la información personal de salud.

Muchos proveedores de Cloud Computing ignoran los datos almacenados por parte de sus clientes; sin embargo, la seguridad e integridad de la información es recomendable manejarlo en conjunto (cliente y proveedor); con una estrategia de seguridad se evitarán casos de violación de la información personal, salud, datos financieros confidenciales, entre otros.

El proveedor de servicios en la nube puede incurrir en multas significativas y daños a la reputación si no se aplican las medidas de seguridad y privacidad adecuadas; en esta parte es donde el diseño e implementación de un **Sistema de Gestión de Seguridad de la Información** con consideraciones específicas y controles seleccionados adaptados a la seguridad y privacidad de la nube que forma parte de nuestros datos, es de gran valor para los clientes.

Adicionalmente en lo referente a seguridad de la información tenemos dos principales preocupaciones:

1) **Pérdida de gobernanza:** Al momento de utilizar una infraestructura en nube, el cliente otorga el control de una serie de actividades que pueden influir en la seguridad al proveedor de la nube. Al mismo tiempo, puede ocurrir que los acuerdos de nivel de servicio (SLAs) no incluyan la prestación de dichos servicios por parte del proveedor en nube, dejando así un vacío en la defensa de seguridad.

   La pérdida de gobernanza y control podría influir gravemente sobre la estrategia de la organización, por lo tanto, sobre la capacidad de cumplir su misión y sus objetivos. Además, podría generar la imposibilidad de cumplir los requisitos en materia de seguridad, la falta de confidencialidad, integridad y disponibilidad de los datos y el deterioro del rendimiento y de la calidad del servicio.

2) **Seguridad técnica:** En este punto es importante destacar que mitigar nuestra preocupación en los aspectos técnicos dependerá de lo que el proveedor y el cliente establecen al momento de adquirir servicios en la nube principalmente en cómo funciona la seguridad en las diferentes capas de la nube, que ofrecen los proveedores de acuerdo a nuestras necesidades y de qué manera evitan o minimizan los riesgos a los cuales se pueden exponer.

2.1.2 Privacidad

Cuando nos referimos a preocupaciones acerca de Privacidad se debe realizar las siguientes preguntas para asegurar que nuestra información no se encuentra en riesgo:

- ¿El proveedor colecta y/o analiza la información del cliente para su propio uso?, en caso de así serlo debe ser reportado al cliente para evitar posible pérdida de información valiosa, entrega de datos relevantes a la competencia o modificación de la misma.

- ¿Es una parte de esa información es cargada o administrada por terceras partes?, los proveedores son dueños de manera total y parcial de nuestra información.

- ¿Es el cliente notificado sobre la recolección de información?, en caso de no serlo el proveedor podría estar incumpliendo políticas y procedimientos preestablecidos por el cliente.

- ¿El cliente es capaz de restringir que datos pueden ser utilizados por terceras partes y/o limitar su uso?, es todo es muy importante porque como empresa se debe estar al tanto de nuestra información y en el estado que se encuentra de manera periódica o en tiempo real.

- ¿Prohíbe el proveedor la transferencia de información personal e identificable?, esto es una gran preocupación porque los proveedores de nube se adueñan de la información incurriendo grandes gastos a la compañía para la entrega de la misma.

Al momento que identificamos que algunas de estas preguntas con una respuesta de diferente, en donde los activos de información se encuentran en riesgo se debería considerar reevaluar el proveedor de nube, acuerdos preestablecidos y nivel de administración de nuestros activos de información.

2.1.3 Confiabilidad

Según Microsoft, en Microsoft Azure la nube parte de la migración mantienen principios de nube de confianza o confiable cumpliendo compromisos de utilizar los datos de los clientes de manera responsable, transparente basado en prácticas de privacidad, y ofrecer privacidad y opciones de control significativas a los clientes.

Los clientes son dueños de sus datos, no el proveedor. Cuando se utiliza un servicio de Microsoft Azure, se mantiene la posibilidad de llevar los datos con el cliente cuando termine el acuerdo. Cuando expira una suscripción o el cliente termine su contrato, Microsoft sigue una política de retención de 90 días y estándares estrictos para sobrescribir el almacenamiento antes de reutilizarlo.

Sus datos no son utilizados para mercadeo. El modelo de negocios empresariales no está basado en explotar los datos de los clientes. No utilizan los datos para propósitos como publicidad que no estén relacionados con brindar el servicio de nube.

No se utiliza acceso vertical. Se ha fabricado servicios de nube para que la mayoría de las operaciones estén automatizadas por completo. Sólo un pequeño conjunto de actividades requiere involucramiento humano; el acceso a los datos por parte de personal de Microsoft está autorizado sólo cuando se requiere algún tipo de soporte u operaciones, luego se revoca cuando ya no se necesita.

Los clientes pueden elegir la ubicación de su centro de datos. Dependiendo de qué servicios de nube de Microsoft tengan, podrán tener flexibilidad en la elección del lugar donde los datos residen de manera física. Los datos pueden ser replicados para redundancia dentro del área geográfica, pero no son transmitidos fuera de ella.

Se protege los datos de la vigilancia gubernamental. Por varios años, se ha expandido la encriptación a través de todos los servicios y reforzado las protecciones legales para los datos de los clientes. Se ha mejorado la transparencia para pueda estar seguro de que en Microsoft no se ofrece productos y servicios restrictivos, ni tampoco se brinda de forma pública el acceso directo o libre a los datos de los clientes.

Microsoft no revelará los datos almacenados a un tercero excepto bajo la solicitud o como sea requerido por ley. Se busca redirigir al dueño de los datos directo cuando se solicitan datos de los clientes.[33]

2.2 Seguridad en Cloud Computing y comparación

La seguridad en Cloud Computing es cada vez mayor que en sus comienzos, su principal prioridad es la información almacenada por sus usuarios finales motivo por el cual las nubes reconocidas tales como Microsoft Azure, Amazon, Google, entre otras sobresalientes se basan en los siguientes puntos para generar confianza e integridad en sus servicios pero sin llegar al nivel de un Sistema de Gestión de Seguridad de la Información (SGSI) se adapta en su totalidad a las necesidades de una compañía específica.

[33] News Center LATAM. (2016). La Nube Confiable: ¿Qué significan en verdad la privacidad y el control?. 2017, de Microsoft Sitio web: https://news.microsoft.com/es-xl/la-nube-confiable-que-significan-en-verdad-la-privacidad-y-el-control/

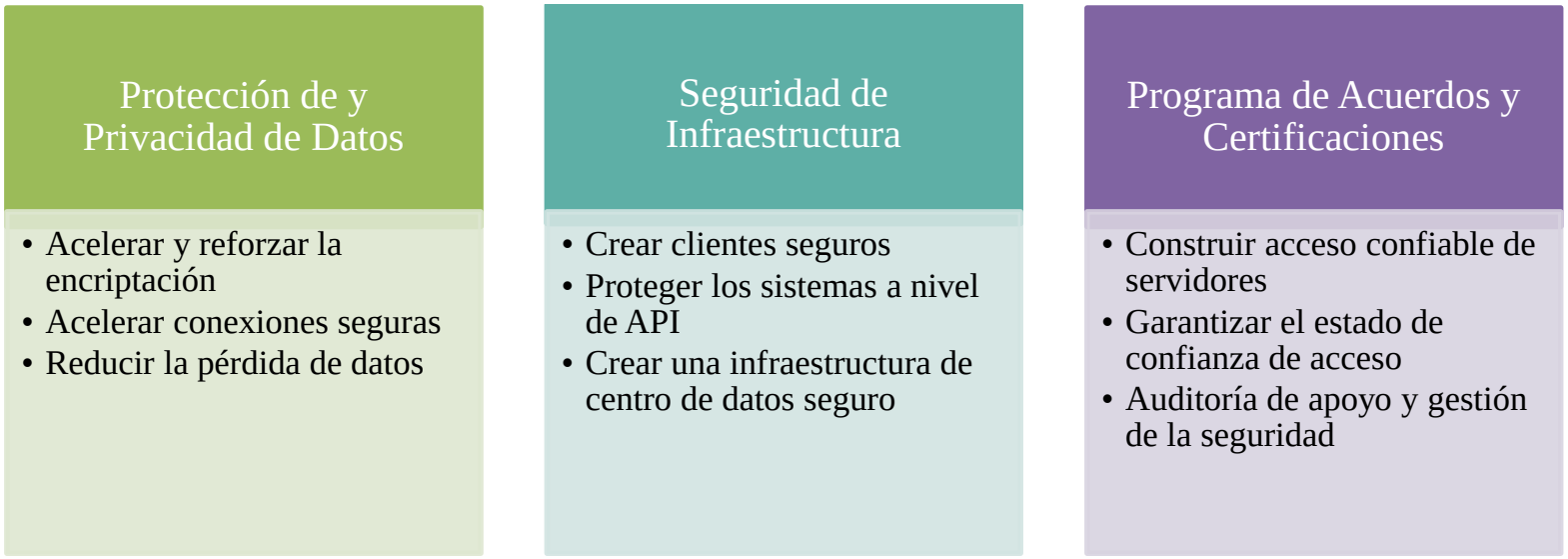


Ilustración 10: Plan de acción de seguridad

Fuente: (EY, 2015)

A continuación, se visualizan los diferentes planes de seguridad que cada uno de los proveedores de nube mantiene, los mismos son recomendados al utilizar normas, metodologías y estándares que lo complementan de mejor manera según los servicios y aplicaciones que se encuentran utilizando:

Proveedor	Identidad y Acceso	Seguridad de Red	Protección de Datos	Privacidad de Datos	Prevención de Amenazas
Microsoft Azure	Sincronización de identidades existentes e inicio de sesión único en Azure, Office 365 y otras aplicaciones en la nube.	Conectarse con seguridad al centro de datos en las instalaciones u ordenador personal mediante Azure Virtual Network	La encriptación se utiliza para ayudar de forma segura al tránsito de datos entre centros de datos y aplicaciones o servicios en Microsoft Azure	Se puede especificar las áreas geográficas donde se almacena los datos, sus datos pueden replicarse dentro de un área geográfica (redundancia)	Sistemas de despliegue integrados administrarán las actualizaciones de seguridad para software de Microsoft, y se puede aplicar la administración de actualizaciones de procesos para máquinas virtuales
	Monitoreo de patrones de acceso para identificar y mitigar las potenciales amenazas	Administrar las máquinas virtuales con el escritorio remoto cifrado y sesiones de Windows con PowerShell	Puede optar por aplicar un cifrado adicional usando una gama de enfoques a controlar por medio de métodos de cifrado y claves	Obtener compromisos contractuales adicionales acerca de la transferencia de datos personales	Seguimiento y análisis de tráfico continuo que revelan anomalías y amenazas forenses por medio de herramientas que permiten análisis minucioso de los ataques

	Ayuda a prevenir el acceso no autorizado con Azure MultiFactor	Mantenga regulado su tráfico de Internet mediante el uso de Azure ExpressRoute, un enlace de fibra privado entre usted y Azure	Si elimina los datos o ya no forma parte de Azure, seguimos estrictos estándares de la industria que sobrescribe los recursos de almacenamiento antes de su reutilización, así como físicamente la eliminación de hardware fuera de servicio	Se limita a Microsoft el acceso y uso de sus datos, se tiene un control estricto y se accede sólo cuando sea necesario para proporcionar o solucionar problemas en el servicio. Nunca utilizamos sus datos de cliente con fines publicitario	Se pueden realizar pruebas de penetración de aplicaciones que se ejecuta en Azure y ocupamos de las pruebas de penetración de los servicios de Azure
Google Cloud	Con las herramientas de Cloud Platform, puede leer las operaciones y registros de acceso para Compute Engine, App Engine, BigQuery, nube de SQL, gestor de despliegue, nube VPN y almacenamiento en la nube	Nube de interconexión y gestionado VPN le permiten crear canales cifrados entre su entorno IP privada en instalaciones ya la red de Google	Cloud Platform proporciona las capacidades fundamentales necesarias para construir aplicaciones seguras	Prevención de los usuarios finales de compartir información crítica fuera de la compañía y brinda la garantía de mantener los datos con seguridad específica y de manera individual	Detección de intrusos Google implica un control estricto del tamaño y la composición de la superficie de ataque de Google a través de medidas preventivas, l empleo de controles inteligentes de detección en los puntos de entrada de datos, y el empleo de tecnologías que remedien automáticamente ciertas situaciones peligrosas.

Amazon AWS	AWS Identity and Access Management (IAM) permite definir cuentas de usuarios individuales con permisos en los recursos de AWS	AWS proporciona varias capacidades y servicios de seguridad para mejorar la privacidad y controlar el acceso de redes.	AWS le ofrece la posibilidad de añadir una capa de seguridad adicional a sus datos en reposo en la nube, proporcionando características de cifrado escalables y eficientes.	La infraestructura de AWS implanta potentes salvaguardias para proteger la privacidad de los clientes. Todos los datos se almacenan en centros de datos de AWS de alta seguridad.	Gran visibilidad en las llamadas de la API a través de AWS CloudTrail, que indica quién realizó la llamada, el tipo de la llamada y el lugar desde donde se hizo
	AWS Multi-Factor Authentication es para cuentas con privilegios e incluye opciones de autentificación basados en hardware	Los firewalls de red integrados en Amazon VPC y las capacidades de firewall para aplicaciones web existentes en AWS WAF permiten crear redes privadas y controlar el acceso a las instancias y aplicaciones	Capacidades de cifrado de datos disponibles en los servicios de base de datos y almacenamiento de AWS, como EBS, S3, Glacier, Oracle RDS,-* SQL Server RDS y Redshift	AWS proporciona diversas API para que pueda integrar el cifrado y la protección de los datos con cualquiera de los servicios que desarrolle o implemente en un entorno de AWS.	Opciones de agregación de logs que simplifican las investigaciones y los informes de conformidad

	AWS ofrece integración nativa con Identity and Access Management en muchos de sus servicios, además de integración de la API con cualquiera de sus propios servicios o aplicaciones.	Cifrado en tránsito con TLS en todos los servicios	Opciones flexibles de administración de claves, como AWS Key Management Service, que permiten elegir si desea que AWS administre las claves de cifrado o si quiere mantener el control total sobre las claves	Almacenamiento de claves criptográficas dedicado y basado en hardware que utiliza AWS CloudHSM y permite satisfacer los requisitos de conformidad	Notificaciones de alerta a través de Amazon CloudWatch cuando ocurren determinados eventos o cuando se superan ciertos umbrales

Tabla 5: Tabla comparativa de planes de seguridad en la nube

Fuente: (Lozada, 2016)

En conclusión, se analizó cuáles son los servicios brindados por los tres proveedores de nube reconocidos que se encuentran bajo una normativa como ISO/IEC 27001, HIPAA, SOC 1, 2 o 3, entre otros, en donde encontramos servicios de autenticación e identificación, seguridad de red, protección, privacidad de datos y prevención de amenazas.

No obstante, la compañía o cliente es responsable de contratar a cualquier consultora para realizar una evaluación que certifique que el diseño o implementación en curso se encuentre alineado con los controles y procesos dentro de la compañía, cumpliendo las normas o estándares seleccionados. Los servicios ofertados bajo la normativa serán efectivos según el tipo de negocio, estrategia o manera de implementación que se desee aplicar.

A continuación, los proveedores reconocidos con sus respectivas certificaciones, leyes, regulaciones y marcos reguladores actualmente implementados en algunos de sus servicios ofertados:

Proveedor	Certificaciones/Acreditaciones	Leyes, regulaciones y privacidad	Homologaciones/ Marcos reguladores
Amazon Web Services	✓ DoDSRG ✓ FedRAMP ✓ FIPS ✓ IRAP ✓ ISO 9001 ✓ ISO 27001 ✓ ISO 27017 ✓ ISO 27018 ✓ MLPS ✓ MTCS ✓ PCI DSS ✓ Norma SEC 17-a-4 ✓ SOC 1 ✓ SOC 2 ✓ SOC 3	✓ CS Mark [Japón] ✓ DNB [Países Bajos] ✓ EAR ✓ Cláusulas modelo de la UE ✓ FERPA ✓ GLBA ✓ HIPAA ✓ HITECH ✓ IRS 1075 ✓ ITAR ✓ Ley My Number [Japón] ✓ DPA de Reino Unido - 1988 ✓ VPAT / Sección 508 ✓ Política de protección de datos de la UE ✓ Ley de privacidad [Australia] ✓ Ley de privacidad [Nueva Zelanda] ✓ PDPA - 2010 [Malasia]	✓ CJIS ✓ CLIA ✓ CMS EDGE ✓ CMSR ✓ CSA ✓ FDA ✓ FedRAMP TIC ✓ FISC ✓ FISMA ✓ G-Cloud ✓ GxP (FDA CFR 21 Parte 11) ✓ IT Grundschutz ✓ MITA 3.0 ✓ MPAA ✓ NERC ✓ NIST ✓ PHR ✓ Principios de seguridad de UK Cloud ✓ Cyber Essentials del Reino Unido

		✓ PDPA - 2012 [Singapur]	
Microsoft Azure	✓ China MLPS ✓ DIACAP ✓ DISA ✓ FedRAMP ✓ FERPA ✓ FIPS ✓ CCSL ✓ ISO 27001 ✓ ISO 27018 ✓ MTCS ✓ NZCC ✓ PCI DSS ✓ Section 508 ✓ Shared Assessments ✓ SOC 1 ✓ SOC 2 ✓ SOC 3 ✓ ENS Spain	✓ PDPA [Argentina] ✓ CS Mark Gold ✓ EU Model Clauses ✓ FERPA ✓ HIPAA ✓ HITECH ✓ IRS 1075 ✓ Ley My Number [Japón]	✓ CJIS ✓ CSA CCM ✓ CDSA ✓ China GB 18030 ✓ China TRUCS ✓ ENISA IAF ✓ FACT ✓ FDA ✓ FISC ✓ FISMA ✓ GXP ✓ MPAA ✓ NIST 800-171 ✓ UK G-Cloud
Google Cloud Platform	✓ SOC 2 ✓ SOC 3 ✓ ISO 27001 ✓ ISO 27017 ✓ ISO 27018 ✓ FedRAMP ✓ PCI DSS	✓ HIPAA ✓ EU Model Contract Clauses	✓ FISMA

Tabla 6: Tabla Comparativa de Acuerdos y Regulaciones de nube

Fuente: (Lozada, 2016)

En conclusión:

1. Amazon AWS cuenta con un total de 15 certificaciones y acreditaciones, 17 leyes, regulaciones y privacidad y 19 homologaciones y marcos reguladores.

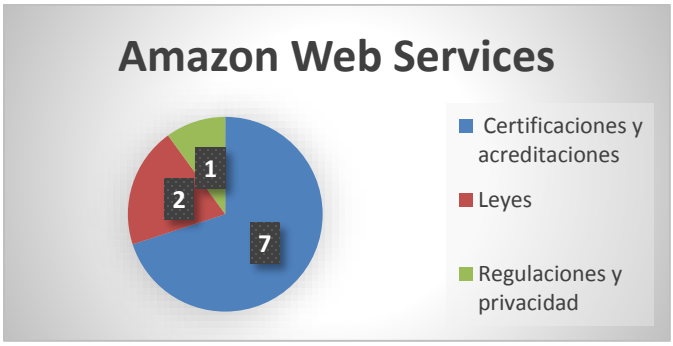


Ilustración 11: AWS análisis de seguridad en servicios Cloud Computing

Fuente: (Lozada, 2016)

2. Microsoft Azure cuenta con un total de 18 certificaciones y acreditaciones, 9 leyes, regulaciones y privacidad y 15 homologaciones y marcos reguladores.

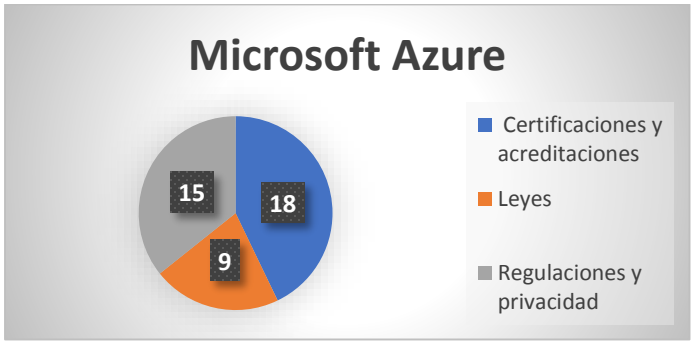


Ilustración 12: Microsoft Azure análisis de seguridad en servicios Cloud Computing

Fuente: (Lozada, 2016)

3. Google Cloud cuenta con un total de 7 certificaciones y acreditaciones, 2 leyes, regulaciones y privacidad y 1 homologaciones y marcos reguladores.

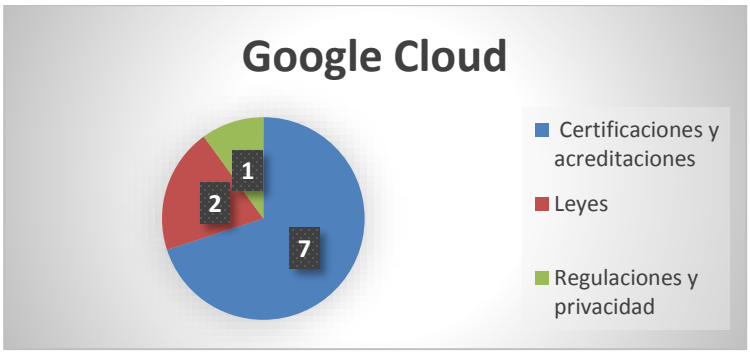


Ilustración 13: Google Cloud análisis de seguridad en servicios Cloud Computing

Fuente: (Lozada, 2016)

No existen servicios o proveedores de Cloud Computing determinados, es recomendable realizar un estudio de negocio previo para la selección de servicios o proveedores específico, según necesidades del negocio, tipo de información, certificados a los cuales desea alinearse la compañía.

Los tres proveedores seleccionados de nube son los más sobresalientes en el mercado, pero no significa que sean los únicos, los mismos disponen distintas certificaciones asegurando que nuestras aplicaciones, activos de información, entre otros servicios en cualquiera de las tres opciones comparadas mantienen un nivel estándar de seguridad, pero adicionalmente es importante tomar en cuenta varios puntos tales como presupuesto a invertir, experiencia de nuestros empleados, riegos, amenazas u orientación del negocio.

Capítulo III: Implementación de esquemas de seguridad

3.1 Sistema de Gestión de Seguridad de la Información (SGSI)

Inicialmente no es comprensible para todos cuando hablamos de un Sistema de Gestión de Seguridad de la Información, por ello es acertado iniciar con la definición de la misma, y lo que comprende.

Un **Sistema de Gestión de Seguridad de la Información** no se refiere a un "sistema", o "aplicación" real que realiza funciones de seguridad de la información; caso contrario es una representación o análisis de eventos dentro de una compañía para abordar los problemas de seguridad de la información. Esto incluye la aceptación de la alta dirección para abordar y mitigar estos riesgos, por medio de la realización de los siguientes procedimientos:

1) Fomentar un enfoque de la seguridad de la información que aliente y motive al personal de toda la organización a estar al tanto de las mejores prácticas de seguridad de la información.

2) Realizar evaluaciones de riesgo adaptadas a las amenazas y vulnerabilidades únicas de su compañía.

3) Búsqueda proactiva de problemas y preocupaciones a través del uso y selección de metodologías.

4) Garantizar que los controles de seguridad se implementen y sean aplicables a los objetivos y al propósito de su compañía.

5) Establecer el compromiso de mejorar continuamente el **Sistema de Gestión de Seguridad de la Información[34].**

Con lo mencionado se podría definir un **Sistema de Gestión de Seguridad de la Información** como una herramienta de gestión que permitirá conocer, gestionar y minimizar los posibles riesgos que atenten contra la seguridad de la información de nuestra compañía, con siglas en español, SGSI, o por sus siglas en inglés, ISMS.

Algo muy importante, se debe tomar en cuenta la diferencia entre seguridad informática y seguridad de la información.

Entonces, la seguridad informática, se refiere a la protección de la infraestructura de las tecnologías de la información y comunicación (TICs); mientras que la seguridad de la información se refiere

[34] Anónimo. (2016). Sistema de Gestión de la Seguridad de la Información. 2017, de http://www.iso27000.es Sitio web: http://www.iso27000.es/download/doc_sgsi_all.pdf

a la protección de activos de información con mayor importancia (bases de datos, documentos, contratos, etc.).

La metodología permitirá analizar y ordenar la estructura de los sistemas de información, facilitando la definición de procedimientos de trabajo y ofrecerá la posibilidad de disponer de controles que permitan medir la eficacia de las medidas tomadas.

La gestión de los riesgos a través de un SGSI va permitir preservar la confidencialidad (implica el acceso a la información por parte de usuarios autorizados), integridad (exactitud y completitud de la información y sus métodos de proceso) y disponibilidad (acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados en el momento que lo requieran) de la misma.

Cuando un **Sistema de Gestión de Seguridad de la Información** basado en la norma ISO/IEC 27001 e ISO/IEC 27018, es una herramienta o metodología sencilla y de bajo coste que cualquier grande, mediana o pequeña empresa puede utilizarla, dichas normas permitirán establecer políticas, procedimientos y controles con la finalidad de mitigar riesgos o amenazas.

El estándar con mayor efectividad en el diseño e implementación de un Sistema de Gestión de Seguridad de la Información es la norma ISO/IEC 27001. La norma ISO/IEC 27001 es útil como un marco de referencia que prácticamente todos los proveedores de servicios basados en la nube o de otra manera lo pueden implementar, además proporciona una multitud de beneficios a las compañías orientadas al diseño e implementación de un Sistema de Gestión de Seguridad de la Información eficaz, pero antes es bueno aclarar dos puntos muy importantes y que merecen ser mencionados:

1) Los potenciales y actuales clientes demuestran interés en su negocio manteniendo su información protegida y a la vez mitigando cualquier tipo de amenaza o vulnerabilidad.

2) Ayuda a las organizaciones a establecer un enfoque preventivo y proactivo para abordar los problemas de seguridad de la información a tiempo en lugar de permitir una mentalidad inversa que generalmente se fomenta por la cultura de auditoría.

El beneficio que gana una compañía al demostrar a sus clientes que se toma en serio la administración de la información es difícil de medir actualmente, sin una previa implementación de KPIs de seguimiento. El ahorro de costos que una compañía puede disfrutar mediante la implementación de procedimientos de respuesta eficaces en caso de un incidente de seguridad es también incalculable.

ISO/IEC 27001 es de gran importancia, especialmente para los proveedores de servicios en la nube que en virtud de su comercio deben tomar la seguridad de la información más en serio. Aquí es donde las organizaciones pueden implementar, además de los requisitos establecidos por la norma ISO/IEC 27001 una serie de medidas para aumentar el nivel de seguridad y privacidad cuando se manejan datos sensibles, como PII. Esta norma se conoce como ISO/IEC 27018.

ISO/IEC 27018, también conocida como ISO / IEC 27018: 2014, se basa en el sistema de gestión de la seguridad de la información de una compañía mediante el establecimiento de un grupo de controles basados en la privacidad que se dedican a proteger las PII, además proporciona un nuevo subconjunto de controles dedicados a la protección de datos personales confidenciales.

Después de considerar lo anterior, en este momento se puede tener más claro que la implementación de un sistema de seguridad de información alineado con ISO/IEC 27001 ofrece valor en todo sentido para una compañía; para los proveedores de servicios en la nube lograr mitigar cualquier preocupación de seguridad y privacidad para sus clientes alineando estos controles con los correspondientes a la ISO/IEC 27018 puede ser la mejor opción que una compañía puede realizar.

A medida que las tecnologías rodean, las amenazas y vulnerabilidades evolucionan.

Un sistema eficaz de Gestión de Seguridad de la Información ofrece a una organización un enfoque proactivo y avanzado hacia la seguridad de la información. Esto es aún más importante dado que las tecnologías de Cloud Computing generan desconfianza al cliente en un principio por preocupaciones de seguridad y privacidad desde su creación; los riesgos y amenazas sólo seguirán aumentando, pero a su vez tenemos la seguridad de que los riesgos y amenazas serán mitigados.

Si representa a un proveedor de Cloud Computing puede ser el momento de considerar cómo su compañía puede beneficiarse implementado Sistemas de Gestión de Seguridad de la Información que alinea sus controles por medio de ISO/IEC 27001 con los objetivos de ISO/IEC 27018.[35]

Según Roberto Arbeláez, Microsoft Chief Security Advisor para las Américas, "La administración de riesgos depende mucho de sus usuarios y la única vulnerabilidad son las diferentes maneras de acceso a la información, aplicaciones e implementaciones, esa es responsabilidad de la empresa, pero los riesgos actualmente ya es un problema sin solución, estos se mitigan al nivel mínimo por medio de proveedores, consultorías y componentes de seguridad que se ofrecen de manera integrada"[36].

Según Rishabh Software, "Las empresas de nube ofrecen un alto nivel de seguridad en distintos aspectos" [37] como lo veremos a continuación:

[35] Alex Hsiung. (2017). A Management System for the Cloud – Why Your Organization Should Consider ISO 27018. 2017, de CSA Sitio web: https://blog.cloudsecurityalliance.org/2017/05/22/management-system-cloud-organization-consider-iso-27018/

[36] News Center LATAM. (2016). Las 7 claves fundamentales para la seguridad tecnológica de una empresa dichas por experto de Microsoft. 2017, de Microsoft Sitio web: https://news.microsoft.com/es-xl/las-7-claves-fundamentales-para-la-seguridad-tecnologica-de-una-empresa-dichas-por-experto-de-microsoft/

[37] Rishabh Software. (2013). Cloud Security (Concerns & Planning). 2016, de Rishabh Software Sitio web: https://infographiclist.files.wordpress.com/2013/10/cloud-security-concerns-planning_51e5282f38682.jpg

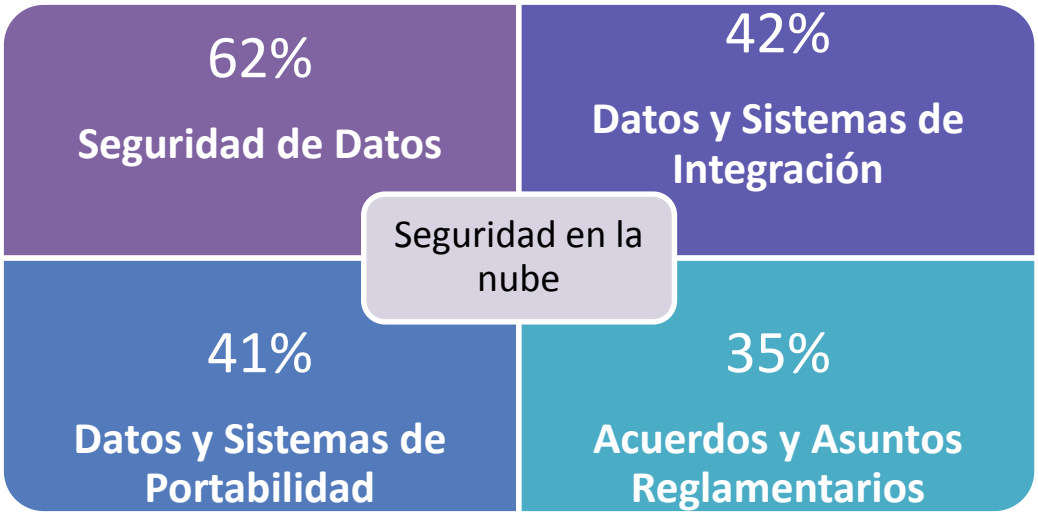


Ilustración 14: Seguridad en la nube

Fuente: (EY, 2015)

De la misma manera que las compañías pueden diseñar e implementar Sistemas de Gestión de Seguridad de la Información de acuerdo a sus necesidades, la mayoría de servicios Cloud Computing se encuentran certificados bajo ciertas normas o estándares utilizando controles preconfigurados.

Para iniciar con la implementación de este modelo, su diseño dependerá de los objetivos y requerimientos de la empresa, así como también de la forma que se encuentra estructurada. En algunos casos no se requiere que en el sistema se involucre a toda la compañía.

La metodología SGSI permite medir y evaluar resultados. Para su implementación se utiliza el modelo PDCA, un modelo basado en el Ciclo de Deming dividido en 4 fases en donde cuando finaliza la última fase y se realiza un análisis de resultados se vuelve a empezar desde la primera.

Las siglas PDCA es equivalente en inglés a Plan, Do, Check y Act (Planificar, Hacer, Verificar y Actuar).

La evaluación continua del Sistema de Gestión de Seguridad de la Información se debe encontrar documentada, para ello se utiliza cuatro tipos distintos de documentación:



Ilustración 15: Cuatro tipos de documentación en el Modelo de SGSI

Fuente: (Lozada, 2016)

En el primer nivel se encuentran el **Alcance** y las **Políticas** que es parte de la base de la seguridad.

En el **Alcance** se indican los lineamientos generales para obtener los objetivos, relaciones, limites que existen entre el alcance y las partes no involucradas de la compañía sin profundizar en detalles técnicos, mientras que las **Políticas** son más alineadas a un documento de contenido genérico que establece los compromisos y en el enfoque de la compañía próxima a implementar un SGSI. Cabe recalcar que la compañía se encuentra en obligación de conocer estas **Políticas**.

En un segundo nivel se encuentra los **Procedimientos** que forma parte de los objetivos de las **Políticas**. Es una de las partes de mayor importancia, en estos documentos se establece una planificación, procesos, flujos del negocios enfocados y control en la seguridad de la información, así como para la medida de la eficacia de los controles seleccionados de los estándares estableciendo métricas. Los **Procedimientos** deben ser conocidos por todas las personas que lo requieran.

En el tercer nivel aparece las **Instrucciones** parte fundamental para el desarrollo de **Procedimientos**, en donde se describe de forma técnica pasos se deben realizar para la ejecución de cada uno de los **Procedimientos**, cuando se habla de procedimientos referimos a: Análisis y evaluación de riesgos, plan de tratamiento de riesgos y procedimientos generales documentados.

Y por último en el cuarto nivel, ubicamos los **Registros** que demuestra la efectiva implementación del sistema y el cumplimiento de los requisitos, entre estos se incluyen indicadores y métricas de seguridad que permiten evaluar la consecuencia de los objetivos de seguridad previamente establecidos.

A continuación, presentamos el Modelo de SGSI, el cual se basa en el Ciclo de Deming (Modelo PDCA):

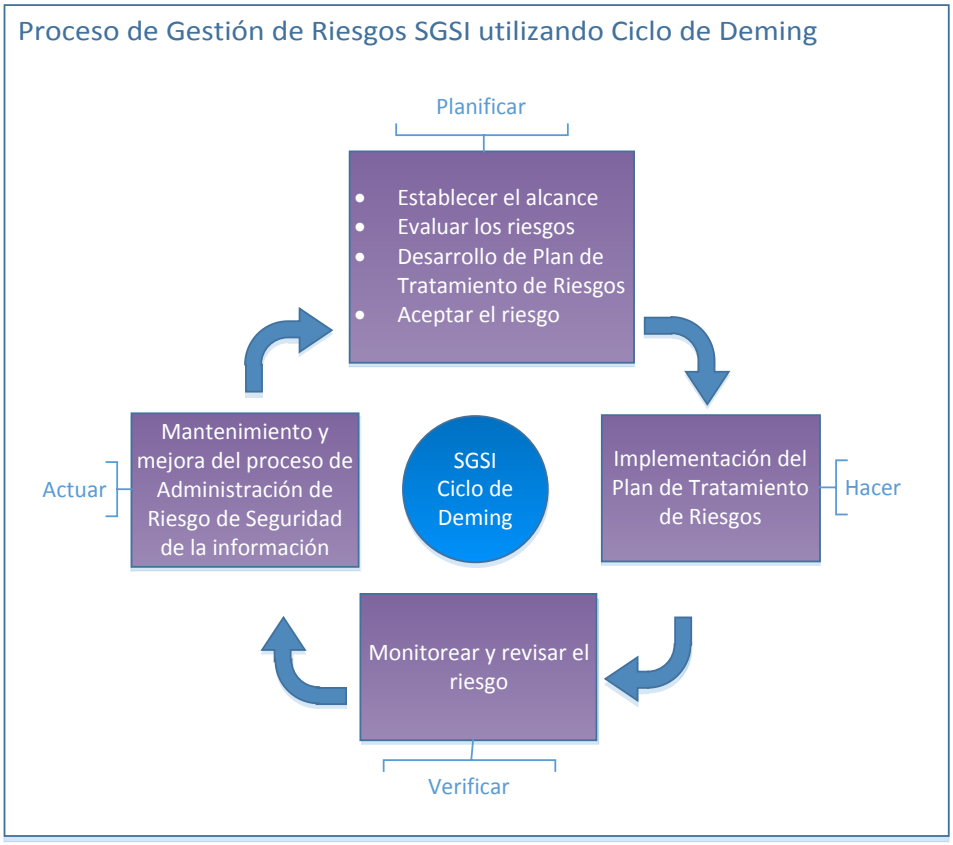


Ilustración 16: Modelo de Sistema de Seguridad de la Información

Fuente: (Lozada, 2016)

La primera fase de Ciclo Deming (Modelo PDCA) para la implementación del sistema es la fase de **Planificación o Planificar.**

Durante esta fase se realiza la **Definición del Alcance** y un estudio de la situación actual de la compañía desde la perspectiva de seguridad, para poder asignar las medidas que se van implementar en función de las necesidades que se detecten.

Se debe tomar en cuenta que no toda la información entregada tiene el mismo valor o se encuentra sometida bajo los mismos riegos y amenazas, para esto es prioritario realizar un **Análisis y Evaluación de Riesgos** para conseguir una solución de mitigación.

Con los resultados obtenidos en el **Análisis y Evaluación de Riesgos** estableceremos controles adecuados para mitigar o minimizar los riesgos y amenazas utilizando los estándares seleccionados: ISO/IEC 27001 e ISO/IEC 27018.

3.2 Implementación de aplicativos en la nube utilizando un SGSI

El uso de servicios en la nube continúa teniendo un importante crecimiento dentro de las organizaciones, principalmente por las ventajas que ofrece, como por ejemplo poder acceder a información o aplicaciones desde cualquier dispositivo que tenga acceso a Internet.

Es importante considerar que esta tecnología en las empresas no solo es utilizada para almacenar información y copias de seguridad, sino también para desplegar aplicaciones y diferentes infraestructuras informáticas. Asimismo, y de acuerdo a un estudio realizado por Gartner que proyecta el estado de la nube entre 2011 y 2016 con respecto a varios aspectos, Latinoamérica no es la región que más ha invertido en términos económicos en esta tecnología (lo es Estados Unidos con el 59%), sin embargo, algunos países de América Latina como Argentina, México y Brasil son las naciones que registran las tasas de crecimiento más altas de servicios en la nube.[38]

Para obtener un despliegue con éxito, es necesario realizar cuatro tareas para establecer una efectiva implementación de nuestro esquema seguridad en nuestros aplicativos en la nube:

1. Desarrollar casos de negocio para apoyar las inversiones en seguridad de la información.

2. Identificar las influencias internas y externas a la organización, por ejemplo, tecnología, entorno empresarial, la tolerancia al riesgo, la ubicación geográfica, y legal y los requisitos reglamentarios.

3. Obtener el compromiso de la alta dirección y el apoyo de otras partes interesadas para maximizar la probabilidad de una implementación exitosa de la estrategia de seguridad de la información.

4. Definir y comunicar los roles y responsabilidades de seguridad de la información en toda la compañía para establecer tareas y líneas claras de autoridad.

   Con el fin de ser eficaz, la gestión de seguridad de información debe proporcionar seis resultados básicos:

   - Alineación estratégica
   - Entrega de valor
   - Gestión de riesgos
   - Evaluación de Riesgos

[38] André Goujon . (2013). La nube continúa creciendo, ¿cómo utilizarla de forma más segura?. 2017, de ESET Sitio web: https://www.welivesecurity.com/la-es/2013/06/25/nube-continua-creciendo-como-utilizarla-forma-mas-segura/

- Administración de recursos

3.2.1 Administración de la información durante la implementación de aplicativos en la nube

Los aplicativos en la nube se basan principalmente en la información entregada por el cliente para ser migrada a la nube por lo que es necesario tomar en cuenta lo siguiente al momento de su transferencia o migración a la misma.

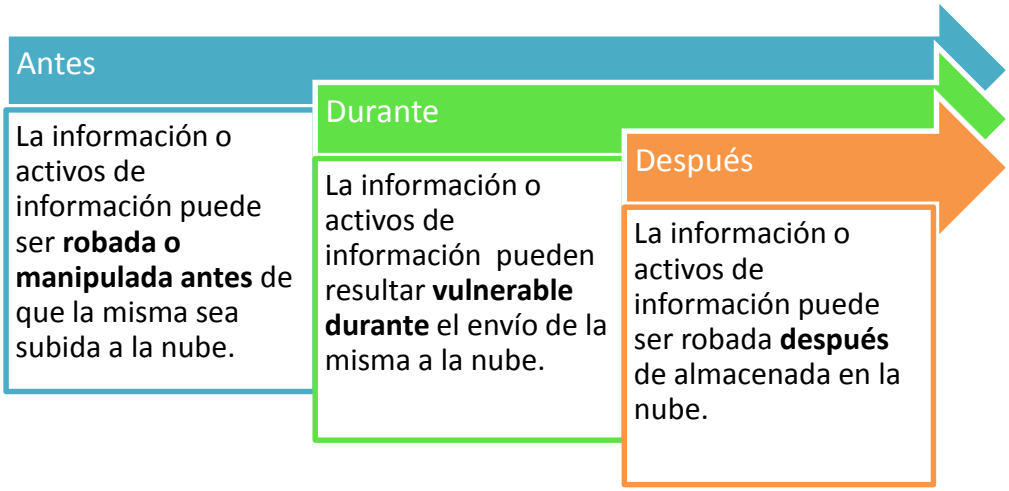


Ilustración 17: Ciclo de vida de seguridad de la información antes, durante y después de la migración a la nube

Fuente: (ESET, 2013)

Según la **Ilustración 15**, en la primera instancia la información podría resultar comprometida antes que esta sea migrada en la nube. Por ejemplo, una organización cuyos sistemas se encuentren infectados con un código malicioso, se expone a que los datos sean robados antes de que sean subidos a la nube. Por otro lado, en la segunda instancia la información también puede correr riesgo si la organización transmite los datos a través de una conexión insegura o sin una autorización previa de entrega. De esta manera, el robo de información ocurriría durante el envío del paquete de información, siendo susceptible, producto de ataques como sniffing o robo de paquetes. En la tercera instancia, la seguridad que adopte el proveedor del servicio en la nube como cifrado de datos, política de uso y seguridad, SGSI, etc., también determina la factibilidad de que la información almacenada en la nube pueda ser vulnerada mediante un ataque en contra del proveedor de los servicios, como sucedido en estos últimos tiempos como, por ejemplo: WannaCry.

Considerando todo lo anterior, se mencionan tres consejos que permiten mitigar los riesgos antes mencionados:

1. Antes de subir la información a la nube: implementar una política de seguridad en la empresa que contemple una protección integral desde los tres pilares fundamentales: tecnología, educación y gestión. De esta forma, el uso de la nube también debe regularse a través de la política de seguridad en lo que respecta a qué datos o sistemas serán almacenados en este tipo de servicios.

2. Durante el envío de información a la nube: en este punto, es importante considerar el uso exclusivo de conexiones a Internet seguras, es decir, que implementen sistemas de protección como un firewall, el acceso restringido a equipos pertenecientes a la empresa, etc. En el caso de conexiones inalámbricas, el uso de WPA2 con cifrado AES, DES entre otros, un SSID oculto, filtrado por direcciones MAC, entre otros, contribuyen a mitigar el impacto de este tipo de ataques.

3. Después de subir la información en la nube: con respecto a esto, documentar correctamente la implementación del SGSI, por ejemplo, el cifrado de los datos almacenados, el uso de doble autenticación como en el caso de Dropbox, la política con respecto a qué se hace cuando la información es eliminada de la nube, etc.

4. Muchas empresas sienten desconfianza al hablar sobre el uso de la nube debido al hecho de que todos los sistemas informáticos son susceptibles de ser atacados por ciberdelincuentes. Asimismo, que los datos se encuentren almacenados en sistemas en los cuales la organización no tiene control directo aumenta todavía más esta desconfianza. Por lo mismo, las medidas que adopten los usuarios y las organizaciones con respecto a la seguridad en la nube son imprescindibles para mitigar las amenazas que atentan en contra de la Seguridad de la Información.

3.3 Metodologías de cifrado

El primer sistema criptográfico del que se tiene conocimiento era conocido como Escítala, este consistía en dos varas del mismo grosor, una en poder del emisor y la otra del receptor. Cuando el emisor quería enviar un mensaje, este, enrollaba una cinta en su vara y escribía el mensaje. De este modo al desenrollar la cinta el mensaje era ilegible. Al recibir el mensaje, el receptor enrollaba la cinta en su vara, y de este modo podía leer el mensaje.[39]

En el transcurso de la segunda guerra mundial la máquina alemana Enigma fue la encriptadora oficial de Alemania.

[39] NA. (2010). La escítala. 2016, de URG Sitio web: http://www.ugr.es/~anillos/textos/pdf/2010/EXPO-1.Criptografia/02a22.htm

El alto mando alemán utilizó como base para la construcción de su máquina los trabajos de Arthur Scherbius, creador de una máquina encriptadora comercial, basada en una serie de rotores que cambiaban una letra por otra. Esta máquina se conocía dentro de la fuerza como “Eins” (Modelo Uno) o “Wermarcht Enigma” (Modelo W) y entró en servicio el 01 de junio de 1930. Era capaz de “mezclar” el texto de los mensajes de 200 quintillones de formas diferentes. Y con la clave correcta, volverlo a la normalidad. Se transformó rápidamente en el código secreto indescifrable de las Fuerzas Armadas.

Los esfuerzos por romper Enigma impulsaron la criptografía y el criptoanálisis de una forma inimaginable. Durante la segunda guerra mundial los aliados finalmente consiguen descifrar Enigma, aunque este hecho se mantiene oculto hasta finales de los años 60.

El 15 de mayo de 1973, el NBS (National Bureau of Standars, en castellano: Agencia Nacional de Normalización) hoy en día denominada NIST (National Institute of Standars and Technology, en castellano: Instituto Nacional de Normalización y Tecnología), hizo un llamamiento en el Federal Register (el equivalente en España del Boletín Oficial del Estado) para la creación de un algoritmo de cifrado que cumpliera con los siguientes requisitos:

- Ofrecer un alto nivel de seguridad relacionado con una pequeña clave utilizada para cifrado y descifrado.
- Ser comprensible.
- No depender de la confidencialidad del algoritmo.
- Ser adaptable y económico.
- Ser eficaz y exportable.

El desarrollo de metodologías de cifrado más seguras se debe a que las empresas necesitaban mantener unas comunicaciones seguras para proteger su información. Por esta razón el gobierno de EEUU y la NSA se ven obligados a crear DES.

A finales de 1974, IBM propuso "Lucifer", que gracias a la NSA (National Standard Agency) fue modificado el 23 de noviembre de 1976, convirtiéndose en **DES (Data Encryption Standard).**

3.3.1 Algoritmos simétricos

Hoy en día, DES se considera inseguro para muchas aplicaciones. Esto se debe principalmente a que el tamaño de clave de 56 bits es corto, las claves de DES se han roto en menos de 24 horas.

Existen también resultados analíticos que demuestran debilidades teóricas en su cifrado, aunque son imposibles en la práctica. Se cree que el algoritmo es seguro en la práctica en su variante de Triple DES, aunque existan ataques teóricos.

Desde hace algunos años, el algoritmo ha sido sustituido por el nuevo AES (Advanced Encryption Standard).

El algoritmo **3DES (Triple Data Encryption Standard)**, se basa en el algoritmo DES, que aplica una serie de operaciones básicas para convertir un texto en otro cifrado, empleando una clave criptográfica. 3DES es el algoritmo que hace triple cifrado del DES, se basa en aplicarlo tres veces con tres claves distintas por lo que resulta mucho más seguro.

En realidad, se dobla la longitud efectiva, siendo de 112 bits, aunque es preciso triplicar el número de operaciones de cifrado, haciendo este método de cifrado muchísimo más seguro que el DES. La longitud de la clave es de 192 bits, aunque como se ha dicho su eficacia solo sea de 112 bits.

Este método está siendo paulatinamente sustituido por el AES, ya que éste tiene una velocidad hasta seis veces más rápida, sin embargo, aún existen medios de pago electrónicos, tarjetas de crédito, etc. que utilizan el estándar 3DES, por lo que continúa estando muy vigente.

El algoritmo **AES (Advanced Encryption Standard)** es uno de los algoritmos más seguros que existen hoy en día. Está clasificado por la National Security Agency (NSA) de EE.UU. para la más alta seguridad de la información secreta. Se basa en varias sustituciones, permutaciones y transformaciones lineales, ejecutadas en bloque de datos de 16 bytes, que se repiten varias veces.

Hasta el momento no existe posibilidad de ataque contra AES, por lo que este algoritmo sigue siendo el estándar de cifrado preferido por gobiernos, bancos y sistemas de alta seguridad de todo el mundo.

El cambio de un solo bit ya sea en la clave o en los bloques de texto simple y claro resulta un bloque de texto cifrado completamente diferente. Algunos criptógrafos muestran preocupación sobre la seguridad porque el número de rondas especificado en el cifrador es muy pequeño y por tener una descripción matemática muy ordenada, y, por lo tanto, predecible.[40]

RC2: Este algoritmo se diseñó para reemplazar al DES y es un algoritmo por clave de tamaño variable de entre 64 y 128 bits que trabaja con bloques de 64 bits y es entre dos y tres veces más rápido que DES. Se puede hacer más seguro que el DES contra ataques de fuerza bruta eligiendo el tamaño de clave apropiadamente.

ICE: Es un cifrado de bloques con clave de 64 bits derivado de DES, sin embargo, ha sido mejorado y diseñado para ser seguro contra el criptoanálisis diferencial y lineal. Su tamaño de clave puede ser cualquier múltiplo de 64 bits, mientras que la clave DES está limitado a 56 bits.

[40] By. (2017). ¿Qué son los algoritmos de encriptación AES y 3DES? 2017, de By Sitio web: https://www.by.com.es/blog/algoritmos-encriptacion-aes-3des/

IDEA (International Data Encryption Algorithm): Algoritmo simétrico que aplica una clave de 128 bits sin paridad a bloques de datos de 64 bits, y se usa tanto para cifrar como para descifrar. Está considerado uno de los más seguros actualmente.

GOST: Es un algoritmo de cifrado de origen ruso que podría ser considerado el análogo ruso al AES. Emplea bloques de 64 bits y claves de 256 bits y no ha podido ser vulnerado a pesar de haber sido uno de los más estudiados. El mensaje de entrada se divide en trozos de bloques de 256 bits (ocho de 32 bits enteros) y el mensaje se rellena añadiendo tantos ceros como se requiere para llevar la longitud del mensaje hasta 256 bits. También se utiliza como función hash.

Serpent: Es un algoritmo de cifrado simétrico de bloques, competidor directo de AES, que usa un tamaño de bloque de 128 bits y soporta tamaños de clave de 128, 192 y 256 bits de longitud. El cifrado consiste en 32 rondas de substitución-permutación operando sobre cuatro bloques de 32 bits. Cada ronda usa 32 copias de la misma S-Box de 4 bit a 4 bit. Serpent se diseñó para que las operaciones se realizasen en paralelo, usando 32 desplazamientos de 1 bit.

Blowfish: Es un codificador de bloques simétricos de 64 bits AES y claves que van desde los 32 bits hasta 448 bits, incluido en un gran número de conjuntos de codificadores y productos de cifrado. Es un codificador de 16 rondas y usa llaves que dependen de las Cajas-S, En total, el algoritmo de cifrado Blowfish correrá 521 veces para generar todas las subclaves, y cerca de 4KB de datos son procesados.

Twofish: Es un algoritmo simétrico con cifrado por bloques de tipo AES. El tamaño de bloque es de 128 bits y el tamaño de clave puede llegar hasta 256 bits. Las características distintivas de Twofish son el uso de S-boxes pre-computadas con llaves dependientes, y una llave-horario relativamente compleja. Es levemente más lento que Rijndael (el algoritmo elegido para AES) para las llaves de 128 bits, pero algo más rápido para las llaves de 256 bits y en muchas ocasiones es más seguro que AES.

RC4: Es el sistema de cifrado de flujo Stream cipher más utilizado y se usa en algunos de los protocolos más populares como Transport Layer Security (TLS/SSL) (para proteger el tráfico de Internet) y Wired Equivalent Privacy (WEP) (para añadir seguridad en las redes inalámbricas). RC4 fue excluido enseguida de los estándares de alta seguridad por los criptógrafos y algunos modos de usar el algoritmo de criptografía RC4 lo han llevado a ser un sistema de criptografía muy inseguro, incluyendo su uso WEP. No está recomendado su uso en los nuevos sistemas, sin embargo, algunos sistemas basados en RC4 son lo suficientemente seguros para un uso común.

RC5: Es un algoritmo de cifrado en bloques desarrollado por Ron Rivest, de hecho, es lo que indican las siglas que dan nombre al algoritmo y en cuanto al número 5 corresponde a una secuencia de algoritmos de cifrado simétrico desarrollados todos por Rivest y que fueron evolucionando (RC2, RC4 y RC5) donde RC5 se dio a conocer en 1995. Este algoritmo salió en sustitución del esquema RC4, el cual había sido publicado anónimamente en Internet. El candidato para AES, RC6, estaba basado en RC5.

3.3.2 Algoritmos asimétricos

ElGamal: Sistema de cifrado asimétrico libre de patentes y utilizado tanto para generar firmas digitales como para cifrar/descifrar. Su funcionamiento se basa en cálculos sobre "logaritmos discretos", factorizando números muy grandes, de 150 dígitos o más. Usa para ello un número primo y dos enteros. La velocidad de cifrado y autenticación es inferior a la obtenida con RSA, las firmas producidas son más largas y los mensajes cifrados ocupan el doble que el mensaje plano.

RSA: El sistema de cifrado asimétrico, que, a diferencia de los anteriores sistemas, trabaja con dos claves diferentes: una clave "pública", y otra "privada". Ambas son complementarias entre sí, así que un mensaje cifrado con una de ellas sólo puede ser descifrado por su contraparte. La longitud de clave va desde los 128 bits a los 4096.

DSA: Algoritmo asimétrico diseñado para las firmas digitales. Ofrece el mismo nivel de seguridad que RSA, aunque está en constante desarrollo debido al apoyo gubernamental.[41]

Diffie- Hellman: Es un protocolo de establecimiento de claves entre partes que no han tenido contacto previo, utilizando un canal inseguro, y de manera anónima (no autentificada). Se emplea generalmente como medio para acordar claves simétricas que serán empleadas para el cifrado de una sesión (establecer clave de sesión). Siendo no autenticado, sin embargo, provee las bases para varios protocolos autenticados.

Su seguridad radica en la extrema dificultad (conjeturada, no demostrada) de calcular logaritmos discretos en un cuerpo finito.

En las últimas décadas, la criptografía con curvas elípticas ha adquirido una creciente importancia, llegando a formar parte de los estándares industriales. Su principal logro se ha conseguido en los criptosistemas basados en el problema del logaritmo discreto, como los de tipo ElGamal. Estos criptosistemas planteados en el grupo de puntos de una curva elíptica garantizan la misma seguridad que los construidos sobre el grupo multiplicativo de un cuerpo finito, pero con longitudes de clave mucho menores.

La criptografía con curvas elípticas aparece como una alternativa a los criptosistemas de clave pública clásicos como el RSA y el ElGamal, tanto por la disminución del tamaño de las claves que se requieren como por el abanico de grupos que ofrecen en el mismo cuerpo base. Su implantación en algunos sistemas de comunicaciones es un hecho constatable y su uso aumenta día a día debido

[41] Devnull. (2016). Algoritmos de Cifrado I. 2016, de El binario Sitio web: https://elbinario.net/2016/04/05/algoritmos-de-cifrado-i/

a sus ventajas. Por ejemplo, se usa en tarjetas inteligentes, sistemas de identificación por radio frecuencia, sistemas de votación electrónica, etc.[42]

3.3.3 Algoritmos Hash

El **SHA (Secure Hash Algorithm, Algoritmo de Hash Seguro)** es una familia de funciones hash de cifrado publicadas por el Instituto Nacional de Estándares y Tecnología (NIST). La primera versión del algoritmo fue creada en 1993 con el nombre de SHA, aunque en la actualidad se la conoce como SHA-0 para evitar confusiones con las versiones posteriores. La segunda versión del sistema, publicada con el nombre de SHA-1, fue publicada dos años más tarde. Posteriormente se han publicado SHA-2 en 2001 (formada por diversas funciones: SHA-224, SHA-256, SHA-384, y SHA-512) y la más reciente, SHA-3, que fue seleccionada en una competición de funciones hash celebrada por el NIST en 2012. Esta última versión se caracteriza por ser la que más difiere de sus predecesoras.

En nuestro caso por Microsoft Azure actualmente cuenta con cifrado de datos transparente (TDE) configurado por medio de comandos en Powershell que utiliza una clave simétrica denominada clave de cifrado de base de datos que protege bien mediante un certificado, el mismo protegido por la clave maestra de la base de datos maestra o bien mediante una clave asimétrica almacenada en una EKM (Encryption Key Management).

La clave maestra de servicio y todas las claves maestras de base de datos son claves simétricas, la metodología de cifrado es sujeta a compatibilidad con Microsoft Azure.

En la **Ilustración 45**, se puede visualizar varias flechas las cuales indican las jerarquías de cifrado comunes. Las claves simétricas y asimétricas de EKM pueden proteger el acceso a las claves simétricas y asimétricas almacenadas en SQL Server. La línea de puntos asociada a la EKM indica que las claves de la EKM podrían reemplazar a las claves simétricas y asimétricas que se almacenan en SQL Server.

Con la creciente demanda de cumplimiento normativo y preocupación por la privacidad de los datos, las organizaciones están aprovechando el cifrado como una forma de proporcionar una solución de "defensa en profundidad". Este enfoque es a menudo poco práctico utilizando sólo herramientas de administración de cifrado de base de datos. Los proveedores de hardware proporcionan productos que abordan la administración de claves empresariales mediante el uso de módulos de seguridad de hardware (HSM). Los dispositivos HSM almacenan claves de cifrado en

[42] Wikipedia. (2017). Diffie-Hellman. 2017, de Wikipedia Sitio web: https://es.wikipedia.org/wiki/Diffie-Hellman#Descripci.C3.B3n_detallada

módulos de hardware o software. Esta es una solución más segura porque las claves de cifrado no residen con datos de cifrado.

El cifrado es más seguro si se incluyen más tipos de cifrado y modalidades entre los que el servidor de bases de datos pueda conmutar. Para obtener información sobre cómo alternar entre cifrados, utilizando frecuencia de conmutación, la cual define cuando se renegocian cifrados y/o claves secretas.

Mientras mayor sea el tiempo que se utilice la clave secreta y el cifrado, más probable será que un atacante rompa las reglas de cifrado. Para evitarlo, los criptólogos recomiendan cambiar periódicamente la clave secreta y el cifrado en las conexiones de larga duración.

Concluyendo el análisis utilizando la información migrada a Microsoft para aplicar todo lo mencionado anteriormente, se ha trabajado en funciones en Transact-SQL utilizando: Claves asimétricas, claves simétricas, certificados y cifrado de datos transparente a través de comandos en Powershell.

Respecto a los algoritmos de cifrado definen transformaciones en los datos que usuarios no autorizados no pueden revertir con facilidad. Actualmente las herramientas en este caso SQL Server permite a los administradores y los desarrolladores de software elegir entre varios algoritmos, incluidos DES, Triple DES, TRIPLE_DES_3KEY, RC2, RC4, RC4 de 128 bits, DESX, AES de 128 bits, AES de 192 bits y AES de 256 bits.

Ningún algoritmo único resulta idóneo para todas las situaciones. Para eso previamente se vio una forma detallada de sus funciones para una selección idónea.

No obstante, se aplican los siguientes principios generales:

- El cifrado seguro suele consumir más recursos de la CPU que un cifrado menos seguro.
- Las claves largas suelen producir un cifrado más seguro que las claves cortas.
- El cifrado asimétrico es menos seguro que el simétrico con la misma longitud de clave, pero es relativamente lento.
- Los cifrados en bloque con claves largas son más seguros que los cifrados de flujo.
- Las contraseñas largas y complejas son más seguras que las contraseñas cortas.
- Si cifra una gran cantidad de datos, debe cifrar los datos con una clave simétrica y cifrar la clave simétrica con una clave asimétrica.

- Los datos cifrados no se pueden comprimir, pero los datos comprimidos se pueden cifrar. Si usa compresión, debe comprimir los datos antes de cifrarlos.

- Adicionalmente para mantener una información segura es necesario el manejo de certificados, un certificado es una instrucción firmada digitalmente que enlaza el valor de una clave pública con la identidad de la persona, dispositivo o servicio que tiene la clave privada correspondiente.

- La entidad que recibe un certificado de una CA es el sujeto de ese certificado. Por lo general, los certificados contienen la siguiente información: La clave pública del sujeto, información que identifica al sujeto, periodo de validez. Es decir, el periodo de tiempo durante el que el certificado se considera válido.

- Un certificado solo es válido durante el periodo de tiempo que se especifica en emismo, estas fechas establecen los límites del periodo de validez. Cuando el periodo de validez de un certificado ha transcurrido, es necesario que el sujeto del certificado expirado solicite uno nuevo.

- El emisor puede revocar un certificado antes de que expire. La revocación cancela las obligaciones que una clave pública tiene con una identidad que se exprese en el certificado.

Capítulo IV: Diseño e implementación de esquema de seguridad en la nube Microsoft Azure

Hoy en día las compañías a nivel mundial, enfrentan distintas amenazas y vulnerabilidades, los cuales si no son detectadas a tiempo se puede llegar a perder grandes sumas de dinero e incluso oportunidades de negocio.

La confidencialidad, integridad y disponibilidad dentro de la compañía es muy importante para que sea gestionada correctamente la información sea o no sensible.

Compañías de varios tipos de industrias, como textil, servicios bancarios, retail, telecomunicaciones, entre otras dependen en gran medida de la información en forma digital para llevar a cabo sus procesos de negocio.

Anteriormente se explicó acerca de las metodologías, marcos y herramientas por utilizarse para mantener un nivel de seguridad estandarizado y eficiente, tomando en cuenta nuestro análisis previo y los datos (activos) entregados para este diseño. Se utilizará las normas ISO/IEC 27001 e ISO/IEC 27018 bajo la metodología de SGSI (Sistema de Gestión de Seguridad de Información).

En el presente capitulo se presentará a continuación nuestro modelo de SGSI, el cual se basa en el Ciclo de Deming (Modelo PDCA):

4.1 Diseño del esquema de seguridad

4.1.1 Planificar

Definición del Alcance

El principal objetivo es fortalecer los servicios y procesos internos. Por medio de mejoras en aspectos relacionados con la seguridad de la información podemos llegar a obtener beneficios a nivel de compañía, proveedores y clientes. Se considerará distintas áreas basándonos en su organigrama identificado roles, dependencias y limitaciones.

La implementación se enfocará en la mejora de seguridad de la información en el proceso de clientes y movimientos, dicho activo es el más importante y uno de los primeros puntos de ataque de robo de información en las compañías en general.

Es importante mencionar que se llevaron a cabo reuniones con personas del área de sistemas en el cual manejarán sus activos por medio de asignación roles según corresponda sus actividades.

A los activos de información o comúnmente llamados datos, se les realizará un análisis y evaluación de los riesgos para identificar los controles que se debe asignar del anexo A de los estándares seleccionados (ISO/IEC 27001 e ISO/IEC 27018), que serían implementados para mitigar cualquier tipo de riesgos.

Se enfocará en los activos de información que se entrega3 en archivos (.txt, xls, bases de datos, documentación de sistemas, procedimientos, manuales, planes de continuidad y soporte).

Cuando se hace referencia a la palabra ‘‘activo’’ su significado conlleva a todo aquello que posee algún valor para la empresa, la cual requiere un tipo de protección o establecer un nivel de seguridad.

Luego de haber determinado el alcance inicial de nuestro SGSI, usualmente es recomendado utilizar el método de las elipses, el cual permitirá primeramente visualizar los distintos subprocesos que forman parte del alcance. Los procesos y subprocesos que forman parte de los clientes, movimientos y servicios ofertados por la compañía seleccionada para la demostración.

Con los usuarios y dueños del proceso, se analizó cuáles son los activos de información más relevantes, para manejarlo bajo una priorización.

Siguiendo la metodología en la segunda elipse se identifica las distintas interacciones que los subprocesos tienen con otros procesos de la compañía, los dueños correspondientes al proceso y los activos de la información involucrados en la interacción. Las flechas permiten indicar las interacciones.

Como tercero y en la última elipse, se identifican aquellas áreas que tienen cierto tipo de interacción con los subprocesos identificados anteriormente. Finalmente, con el método de las elipses se identificó tipos de activos de información existentes dentro del alcance del modelo, basándose en sus procesos, organigrama y datos.

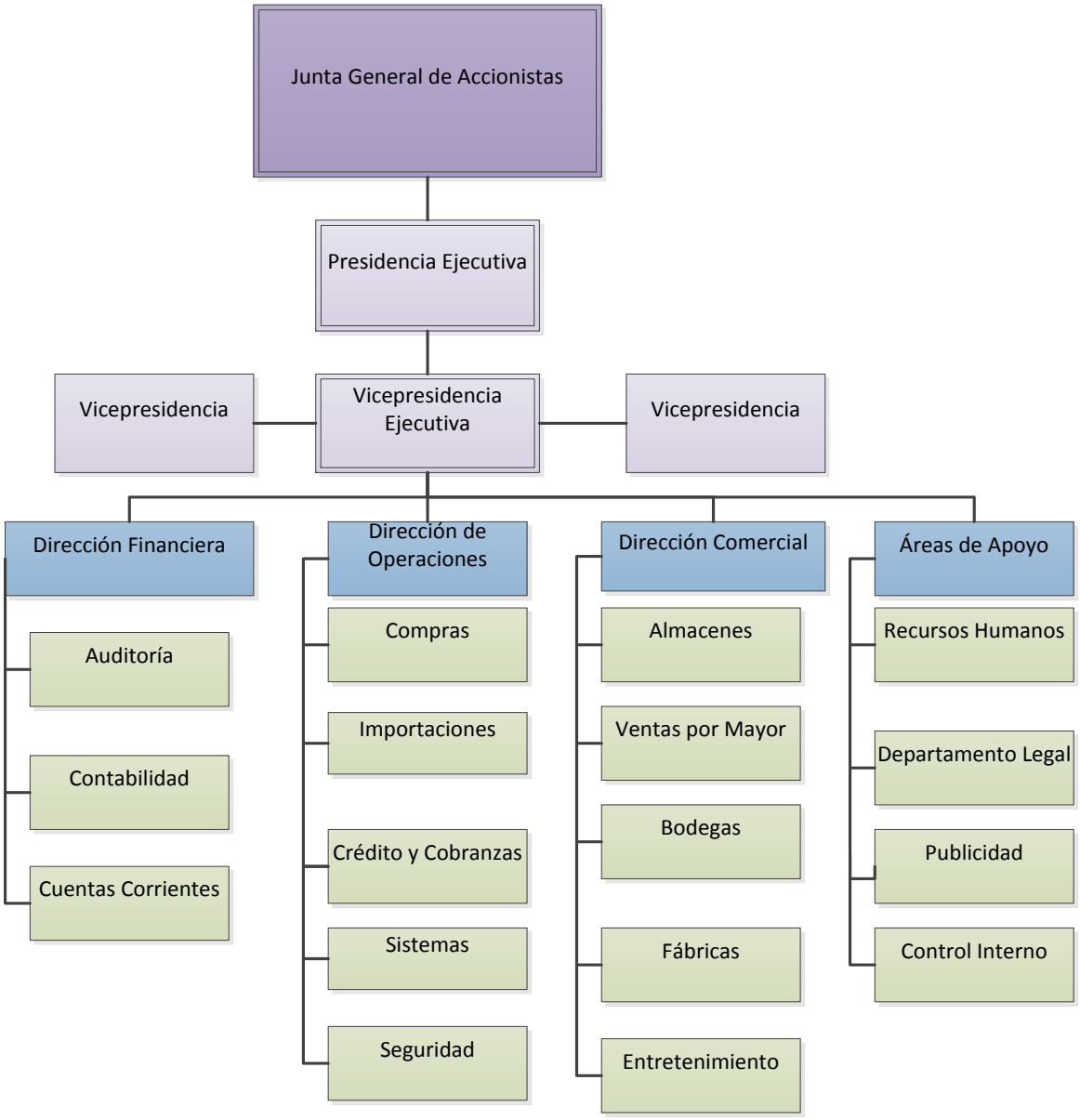


Ilustración 18: Organigrama de la compañía (Empresa parte del estudio de Microsoft Ecuador)

Fuente: (Microsoft Ecuador, 2017)

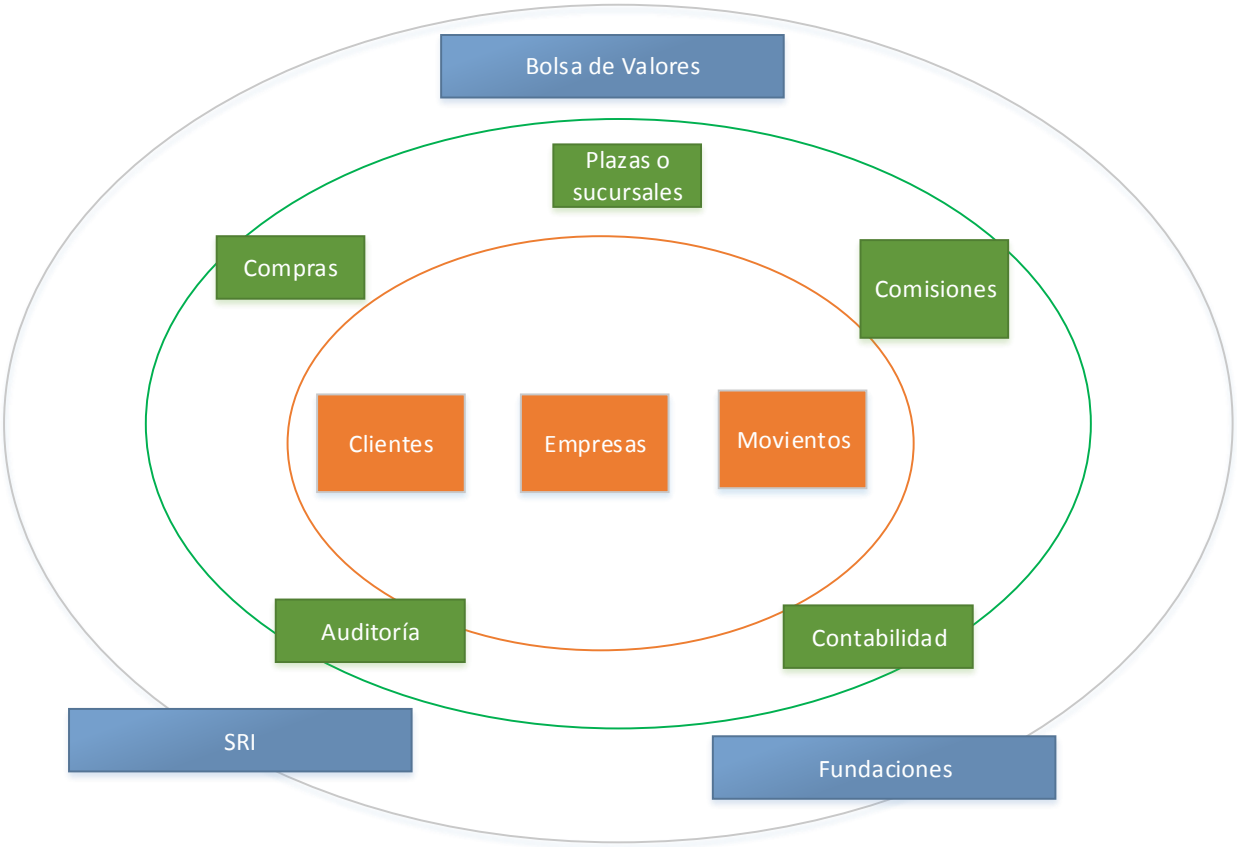


Ilustración 19: Metodología de las Elipses

Fuente: (Lozada, 2016)

Políticas

Es un documento requerido para el desarrollo del SGSI. Son la orientación o directriz que debe ser divulgada, entendida y acatada por todos los miembros de la organización, en ella se contemplan las normas y responsabilidades de cada área de la organización.

Son lineamientos generales a observar en la toma de decisiones sobre algún problema que se repite una y otra vez dentro de una organización. En este sentido, las políticas son criterios generales de ejecución que complementan el logro de los objetivos y facilitan la implementación de las estrategias.[43]

[43] Mariana Medina. (2012). Política organizacional. Concepto y esquema en la empresa. 2017, de Gestiopolis Sitio web: https://www.gestiopolis.com/politica-organizacional-concepto-y-esquema-en-la-empresa/

Dichas políticas y procedimientos fueron determinadas al momento de escoger Cloud Computing como parte de sus aplicaciones y almacenamiento, esta información de conocimiento es aplicada en la compañía, que también involucra a externos que tiene acceso a ciertos niveles de información.

A continuación, se incluye a detalle cada una de ellas:

Políticas	
Nro.	Descripción
1	Las capacitaciones son obligatorias al momento de asignar responsabilidades, esto se realiza cuando el empleado ingresa a la compañía o si el mismo cambia de puesto o asignaciones.
2	Una vez que el empleado es contratado, de manera obligatoria deber aceptar los niveles de confidencialidad de información por cada una de las responsabilidades que vaya a mantener con la compañía
3	Para mantener la integridad y disponibilidad de la información almacenada en nube, en sitio, servidores locales, entre otros es necesario acatarse a las medidas de seguridad establecidas.
4	Todo empleado al momento de ingresar a las aplicaciones e información solo podrá hacerlo con el usuario y contraseña entregado y asignado según sus responsabilidades. Dichas asignaciones son eliminadas al momento de aprobarse una baja de usuario.
5	La compañía debe acatarse al cumplimiento de la ley de protección de datos, según el artículo 4 de la Ley del Sistema Nacional de Registro de Datos Públicos donde dice “las instituciones del sector público y privado y las personas naturales que actualmente o en el futuro administren bases o registros de datos públicos, son responsables de la integridad, protección y control de los registros y bases de datos a su cargo”. Además, se debe asegurarnos que cualquier tercero o externo tenga en cuenta de igual manera el cumplimiento de esta ley para proteger la información adecuadamente.
6	Se deberá mantener cautela y profesionalismo en lo que se refiere a información de carácter confidencial.
7	La información del personal de la compañía es de carácter confidencial. Según el artículo 178 del Código Orgánico Integral Penal.

4.1.2 Análisis y Evaluación del Riesgo

El Análisis y Evaluación del Riesgo es un punto de la metodología donde se identifica, categoriza y valora los eventos que puede ser amenazas para la compañía, cuando se los identifica seleccionando los controles de manera correcta y alineada se puede llegar a mitigar o reducir su impacto de ataque.

Una vez que tenemos definidos los activos de la información involucrados en el alcance por medio de la metodología de las elipses, se procede a establecer el SGSI (Sistema de Gestión de Seguridad de la Información), siguiendo paso a paso los estándares ISO 27001:2013 e ISO 27018:2014, para ello se debe realizar de manera disciplinada y sistemática un análisis y evaluación de riesgos a los activos encontrados para determinar cuáles necesitan ser protegidos para mitigar su riesgo, así como también se debe determinar el riesgo residual (el riesgo que la compañía puede sobrellevar).

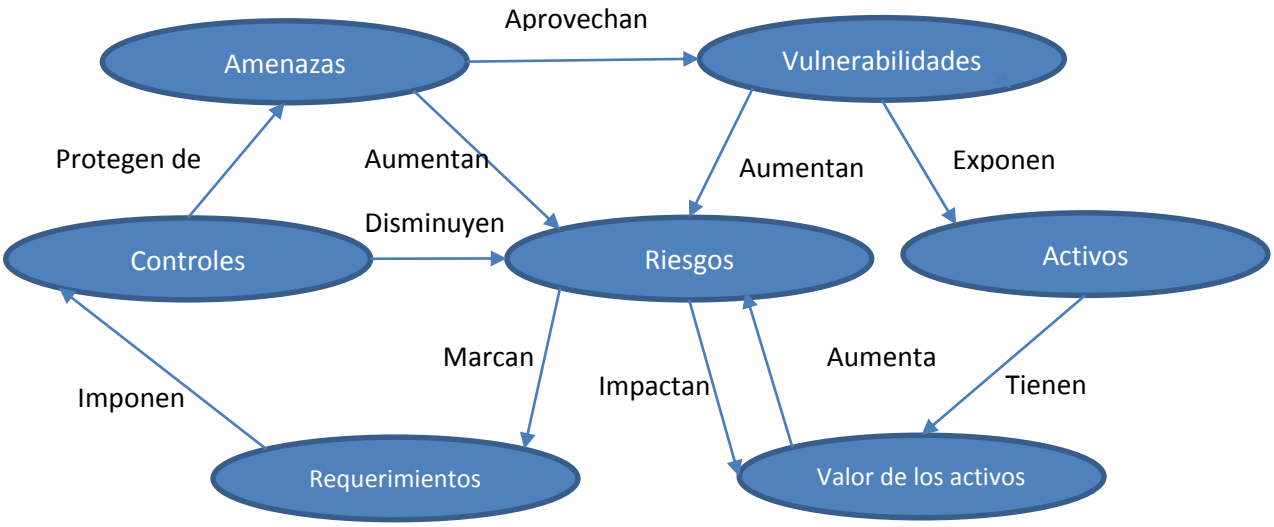


Ilustración 20: Análisis de Riesgos (Metodología basado en papeles obligatorios ISO 27001 e ISO 27018)

Fuente: (Lozada, 2016)

A continuación, se mostrará los pasos a seguir para el manejo de la metodología de análisis y evaluación del riesgo para cumplir las exigencias de los estándares aplicados.

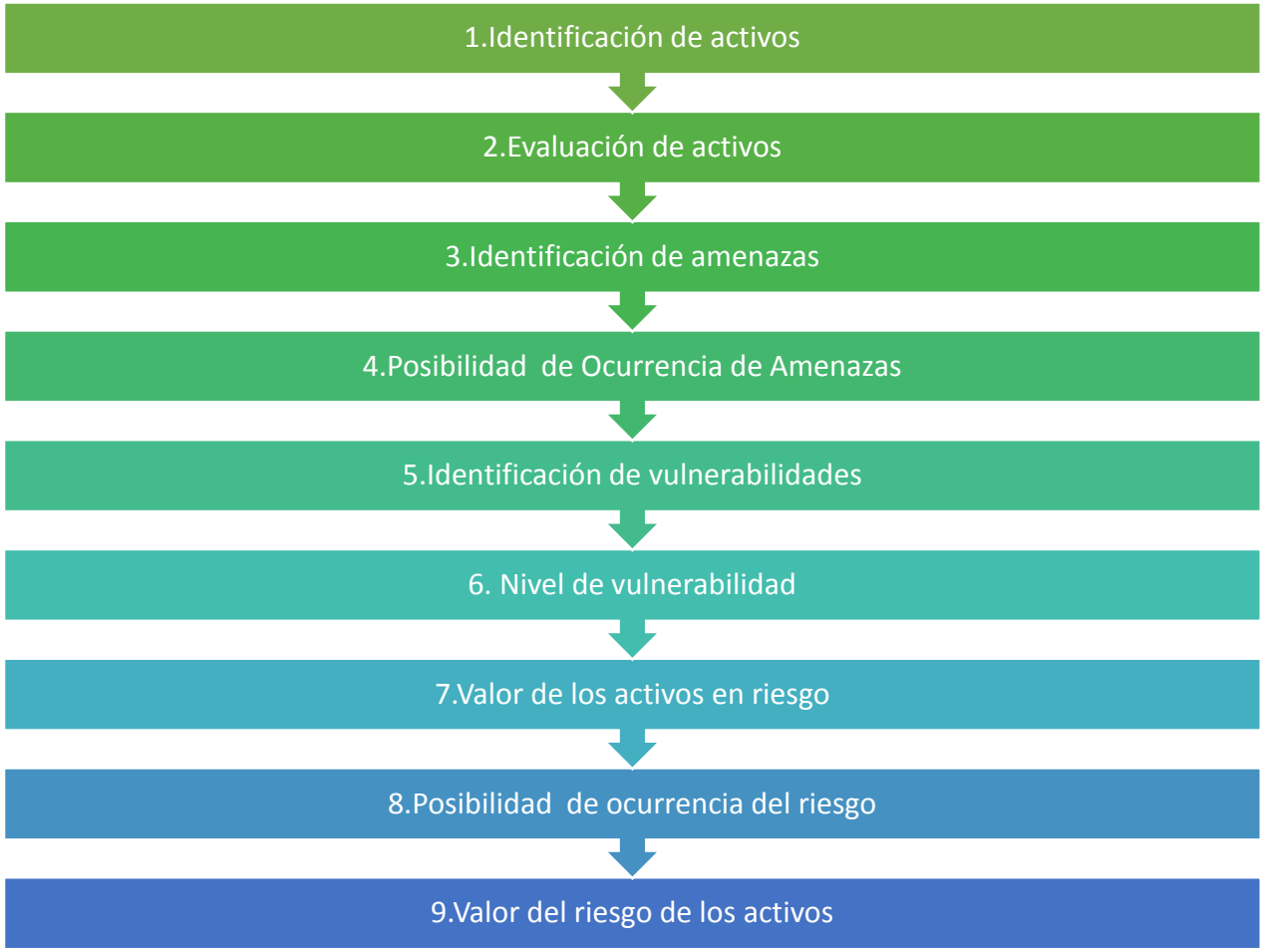


Ilustración 21: Metodología para el Análisis y Evaluación del Riesgo

Fuente: (Lozada, 2016)

Descripción de los activos identificados:

Activo 1 – Estados de cuenta como documento: Bases de datos transaccionales consolidados que mantienen los registros de compras realizadas, depósitos, retiros por medio de ATM, transferencias web, transferencias al exterior, cálculo de comisiones, información de cuenta bancaria en forma general.

Para la administración y acceso a la base de datos, se lo realiza por medio de conexión a internet para acceder al servidor configurado en la nube (Microsoft Azure) para el almacenamiento de información.

El acceso solo es otorgado si la IP del equipo que accede se encuentra registrada y cuenta con un usuario y contraseña según sus responsabilidades asignadas.

Los datos pueden ser visualizados por externos de la compañía para análisis o auditorías en modo de lectura, según el nivel de detalle que se lo necesite.

Activo 2 – Datos del cliente: Base de datos que contiene información completa y confidencial del cliente, la cual debe ser administrada con alto cuidado y reserva. Esta base se encuentra sujeta a la aplicación de las políticas entregadas a la compañía al momento de la adopción de la nube.

Activo 3 – Movimientos diarios: Base de datos próxima migrar al servidor de prueba, la información actualmente se encuentra en formato Excel y es utilizada para el control de cálculo de interés de cuentas de ahorro de todo tipo, así como también el cálculo de interés de sobregiro en cuentas corrientes.

Activo 4 – Medios de Comunicación: Base de datos entregas a externos para cumplimientos de proyectos, transferencia de información entre áreas o entrega de información a otros organismos por motivos de análisis o auditorías, los antes mencionados deben ser capacitados con las políticas de la compañía y acatarse a ella para la manipulación correcta de la información de la compañía.

	Evaluación de Activos			
Activo	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Total**
Estados de cuenta como documento	Alto	Alto	Alto	Alto
Datos de Clientes	Alto	Alto	Alto	Alto
Movimientos diarios	Alto	Alto	Alto	Alto
Medios de comunicación o entrega de información	Alto	Alto	Alto	Alto
Datos en otros formatos .xls, .txt, etc.	Bajo	Alto	Alto	Alto

Tabla 7: Identificación y Evaluación de Activos (Metodología basado en papeles obligatorios ISO 27001 e ISO 27018)

Fuente: (Lozada, 2016)

Activo	Amenazas	Posible ocurrencia	Vulnerabilidad	Posible nivel de vulnerabilidad	Valor activo	Posible ocurrencia	Total
Estados de Cuenta como documento	Falsificación	M	Deficiencia en los formatos de envió	M			
	Pérdida del documento	A	Datos incompletos	A			
	Retraso en la entrega	A	Desconocimiento de extracción segura, o rutas de envió	A	A	M	M
	Ilegibilidad de datos	B	Deficiencia en impresión	B			
	Carga de datos incorrecta	M	Errores de procesamiento en los datos	M			
Datos de Clientes	Plagio	B	Deficiencia en personal que administra la información	B			
	Falsificación	A	Deficiencia en él envió de información	A	A	M	M
	Alteración	A	Acceso a la información por	A			

			personas no autorizadas				
	Privacidad	M	Control de documentos	M			
Movimientos Diarios	Plagio	M	Datos sin respaldos	A			
	Falsificación	M	Ocultar evidencia a las posibles auditorías por llevar doble contabilidad	M	A	M	M
	Pérdida de datos en un sistema informático o base de datos	M	Incorrecta manera de manipulación de datos	B			
Medios de comunicación o entrega de información	Falla funcionamiento	A	Problemas técnicos: Fallas eléctrica, falta de mantenimiento	M			
	Falla seguridad	A	Faltas políticas, estándares	A	A	M	M
	Falta de capacitación al personal	A	Mala administración de la información por los empleados no capacitados	M			
	Plagio	A	Deficiencia en personal que	M			

Datos en otros formatos .xls, .txt, etc.	Falsificación	A	administra la información Datos sin respaldos	M	M	M	M
	Retraso en entrega	M	Incorrecta generación de información	A			

Tabla 8: Análisis y Evaluación de Riesgo iniciales (Metodología basado en papeles obligatorios ISO 27001 e ISO 27018)

Fuente: (Lozada, 2016)

4.1.3 Seguridad de la información en los activos de la compañía seleccionada

Para reducir los riegos y amenazas que fueron analizados y evaluados en la tabla anterior, al igual que la mayoría de aspectos de la gestión empresarial, la gestión de la seguridad de la información depende de las personas que forman parte de la compañía. Los activos de información generan valor cuando es asignada a las personas adecuadas.

Aunque no parezca importante, uno de los procesos fundamentales correspondiente a los empleados de cualquier organización es el de **Reclutamiento** (asignación de roles y responsabilidades).

Cuando un empleado ingresa a la compañía tiene asignado una serie de tareas y responsabilidades, por la cual se le proporciona las herramientas e información necesaria, se debe seguir un proceso con el fin de mantener una estrategia de seguridad de la información sólida. Es común en la mayoría de organizaciones contar con acuerdos o políticas para los activos de información de gran importancia.

4.1.3.1 Asignación de roles y responsabilidades

Los accesos a la información y servicios de Cloud Computing los realiza el departamento de sistemas y seguridad, la asignación de roles y responsabilidades debe ser según su puesto y privilegios para aprobarlos.

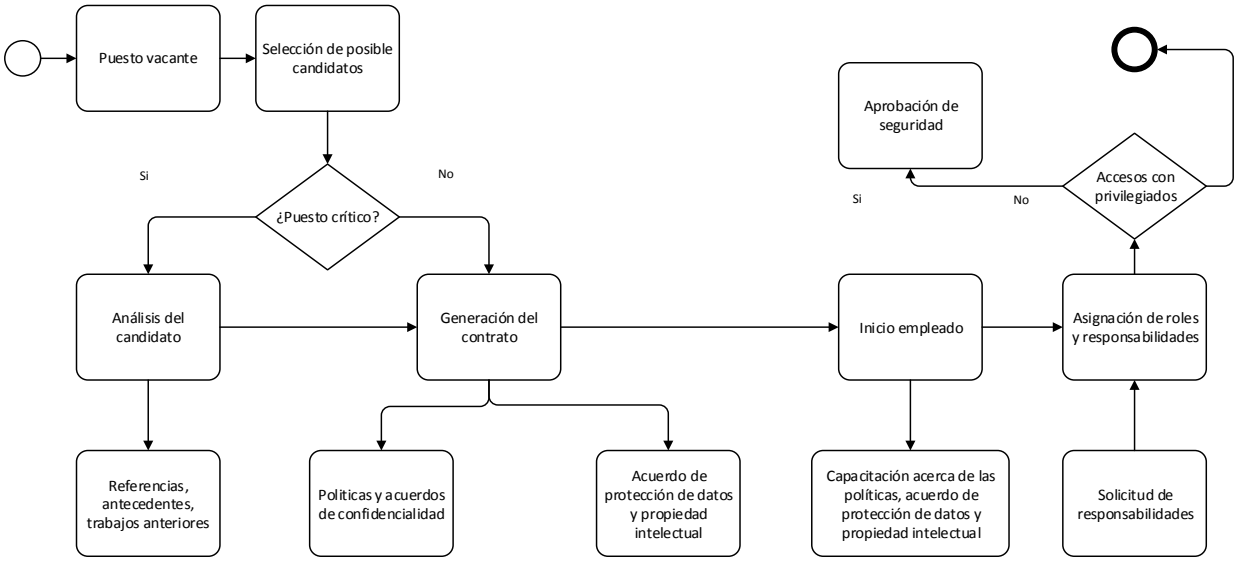


Ilustración 22: Proceso de reclutamiento (asignación de roles y responsabilidades)

(Lozada, 2016)

4.1.3.2 Eliminación de roles y responsabilidades

La eliminación es crítica para la compañía, en caso de que este sea por motivo de despidos o problemas laborales, debido a que existen historias de robo masivo de información sensible, entrega de datos a externos o sabotaje por parte de empleados molestos.

En muchas ocasiones no existe un plan de bajas de usuarios que gestione de manera coordinada y oportuna, el empleado puede seguir durante meses activo en el sistema cuando lo correcto es a partir del día de la salida o más tardar un día después.

Tipos de bajas de usuarios: El responsable del empleado en conjunto con el área de Seguridad de la Información deben especificar las razones que rodean la baja. Las categorías de baja de usuarios son:

- Renuncia
- Despido inesperado
- Despido planificado
- Jubilación obligatoria
- Jubilación anticipada

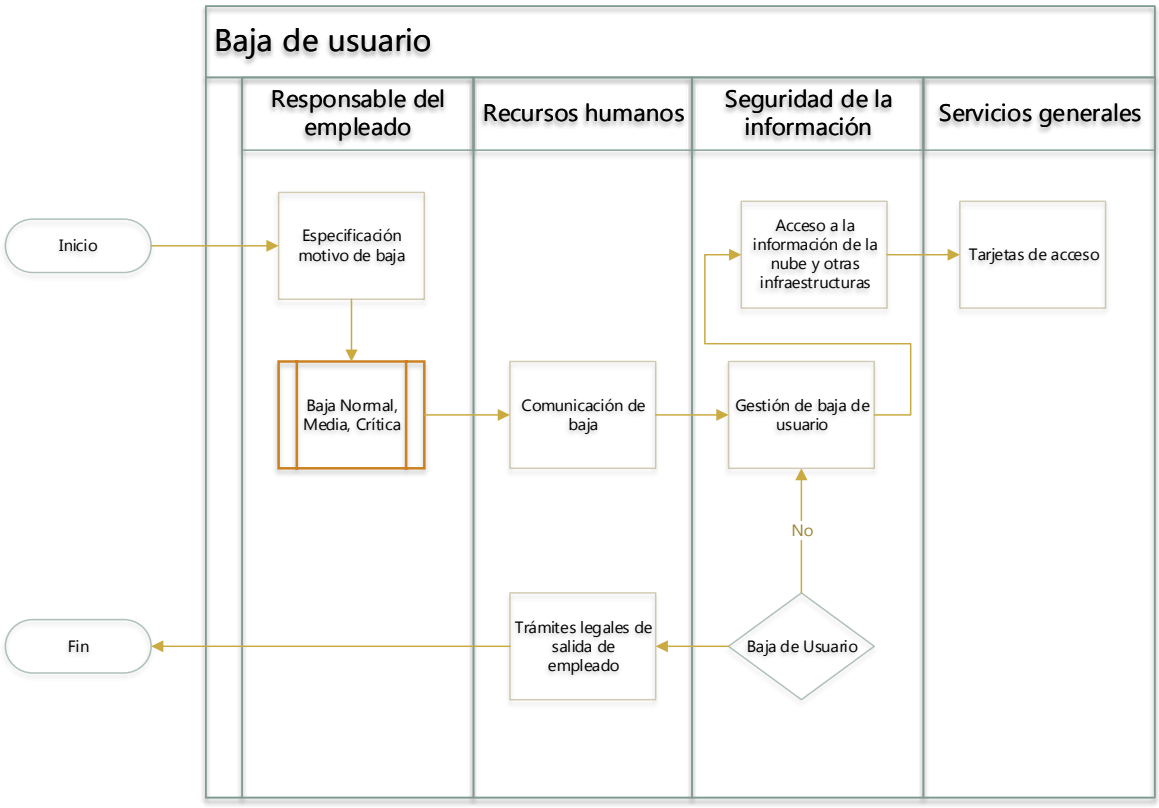


Ilustración 23: Baja de usuarios en la compañía

(Lozada, 2016)

El Sistema de Gestión de Seguridad de la Información será capaz de proteger la información de la compañía cuando los empleados terminen sus funciones, o están sean actualizadas, bloqueando su acceso o eliminando privilegios otorgados en la nube.

El primer paso que se siguió fue la **Identificación de Activos**, para esto utilizamos la metodología de las elipses, en donde se identificó seis activos de información importantes.

Luego se procedió con la **Evaluación de Activos**, el objetivo de realizar este paso es para poder identificar la protección apropiada a los activos, además es necesario que tengan una valoración según su importancia en la empresa.

Se enfocará en los activos de información del proceso de "Estados de Cuenta como documento", en donde se evaluó en relación a su confidencialidad, integridad y disponibilidad manejando niveles cualitativos: Alto, Medio y Bajo. Una vez realizada la evaluación se procedió con la **Identificación de Amenazas**, conociendo que una amenaza es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema

en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio (DoS), en la compañía y sus activos.[44]

Se realizó un análisis de sus activos, con sus posibles amenazas por cada activo de información obtenido en los puntos anteriores.

El siguiente paso es establecer la **Posibilidad de Ocurrencia de Amenazas,** no todas las amenazas tienen la misma probabilidad de ocurrencia, eso depende de sucesos anteriores.

Por cada una de las amenazas se analizó con el área de TI por medio de escalas la posibilidad de ocurrencia basándonos en su experiencia y conocimiento de cada uno de los activos.

Continuando con la metodología, se procedió con la **Identificación de Vulnerabilidades,** las vulnerabilidades es todo aquello que no ha sido considerado en la protección de los activos, son las debilidades que tienen los bienes y que pueden ser explotadas por una amenaza.[45] En donde se analizó y estableció por cada amenaza las vulnerabilidades relacionadas con cada uno de los activos de información. A continuación, se identificó la **Posibilidad de la Vulnerabilidad**, evaluando por cada una de las amenazas.

El paso siguiente de la metodología es la evaluación del riesgo. El riesgo será evaluado por medio de un promedio del **Valor del Activo en Riesgo**, esto es fundamental para evaluación de los riesgos, con esto se enfocará en la pérdida o afectación económica que el riesgo pudiera causar en los activos de información. En el caso de los activos de información de Ventas se realizó un estimado establecido.

4.1.3.3 Posibilidad de Ocurrencia del Riesgo

Por cada activo, amenazas y vulnerabilidades, se determinó la probabilidad de ocurrencia del riesgo por cada activo de información determinado.

Finalmente se establece el **Valor del Riesgo de Activos,** según el análisis y siguiendo la metodología, se concluyó que los activos de información:

Factura como documento, diarios contables y medios de comunicación o entrega de información son los activos de información que se consideran en riesgo por lo tanto serán aquellos que se analizarán con el Anexo A para asignación de sus respectivos controles.

---

[44] Symantec. (2015). Glosario de Seguridad. 2016, de Symantec Sitio web: www.symantec.com/es/mx/theme.jsp?themeid=glosario-de-seguridad

[45] Vulnerabilidades. 2016, de Red y Seguridad Sitio web: http://redyseguridad.fi-p.unam.mx/proyectos/buenaspracticas/vulnerabilidades.html

4.1.3.4 Tratamiento del riesgo

Según la cláusula que se encuentra en ISO/IEC 27001 4.2.1 hace referencia que se deben seleccionar controles apropiados según el Anexo A.

En donde el primer paso fue analizar la probabilidad de riesgos que influyen en la seguridad de la información, teniendo un mejor entendimiento y contexto de la compañía basándonos en: recursos disponibles, procesos organizacionales, estructura organizacional, cultura de la compañía, entre otros.

Una vez que se ha realizado el análisis y evaluación de riesgo, se seleccionó varios activos de información en donde deseamos mitigar el riesgo.

1) Estados de cuenta como documento
2) Movimientos diarios
3) Medios de comunicación y entrega
4) Datos de clientes

El criterio por el cual se escogió estos activos para aplicar los controles apropiados del Anexo A fue la importancia que estos tienen para la empresa, como también el resultado de **Alto Riesgo** en la posibilidad de ocurrencia.

4.1.3.5 Enunciado de aplicabilidad

Según la cláusula 4.2.1 se exige que se documente un "enunciado de aplicabilidad" y en la cláusula 4.3.1 se considera un documento importante durante el desarrollo del SGSI.

El enunciado de aplicabilidad es un documento que hace referencia a los objetivos de control y los controles seleccionado, así como las razones de selección, también se debe adjuntar las razones por que ciertos controles del Anexo A fueron excluidos, este documento importante de SGSI, sirve para demostrar a terceros los motivos al haber escogido ciertos objetivos de control y controles para mitigar los riesgos identificados en los activos de información de la compañía.

El enunciado de aplicabilidad se encuentra en el capítulo de **Anexos (Anexo 1)** al finalizar el presente documento.

4.1.4 Hacer

Anteriormente se menciona que utilizaremos un proceso de implementación basado en el Ciclo Deming que se compone de las fases: Planificar, Hacer, Verificar y Actuar, estos cuatro puntos son de gran importancia para nuestro diseño de seguridad, e iremos detallando de forma detenida los que se realizará, como los que están por realizar en los próximos capítulos.

Fase 1: Planificar

En esta fase se establecerá el alcance, la evaluación de los riesgos, desarrollo de plan de tratamiento de riesgos, aceptación de riesgos y selección de controles del Anexo A en los estándares de seguridad seleccionados para mitigar cada uno de estos posibles riesgos. Se seleccionó el proceso "Movimientos de pasivos" y se realizó un estudio para determinar y escoger los activos más vulnerables a los cuales se aplicaron varios controles de los estándares ISO/IEC 27001 e ISO/IEC 27018 para mitigar el riesgo previamente evaluado o detectado.

A continuación, se muestra el flujograma de Proceso de Planificación utilizado en la primera etapa de la metodología establecida:

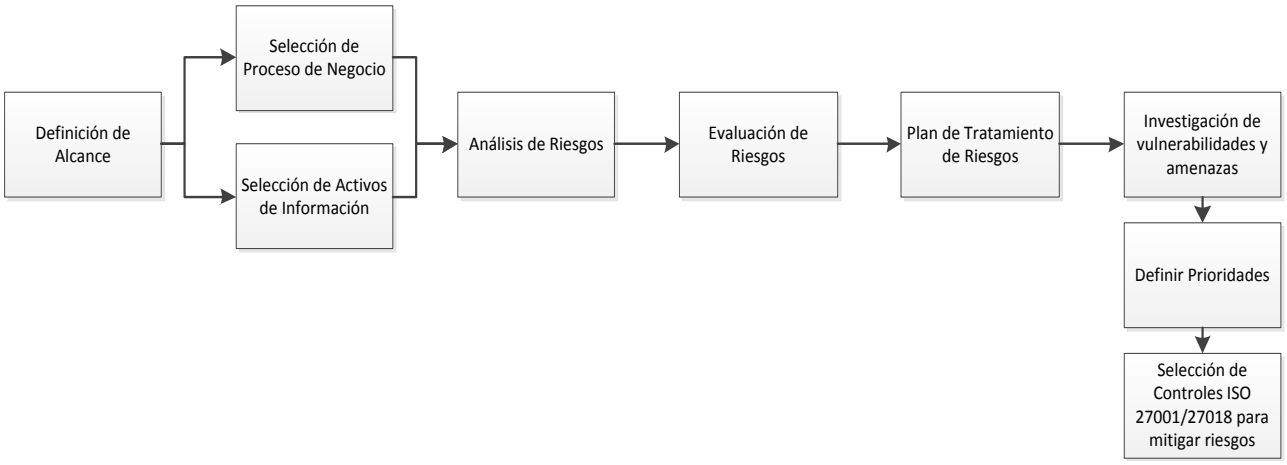


Ilustración 24: Proceso de Planificación SGSI

Fuente: (Lozada, 2016)

Fase 2: Hacer

Esta es la fase actual donde se realiza un esquema de cada uno de los procesos de una forma preliminar basándonos en él análisis de información previa para definir el diseño de la arquitectura a implementar en la nube, diseño de procesos y esquema de información de proceso seleccionando aplicando la metodología y estándares escogidos previamente.

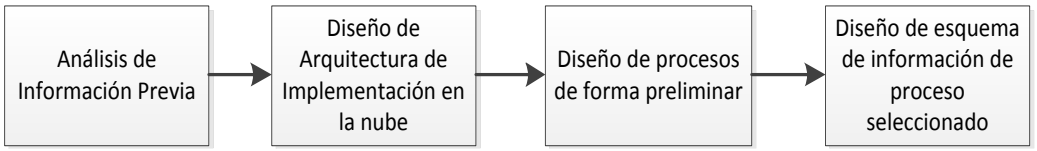


Ilustración 25: Proceso de Hacer en SGSI

Fuente: (Lozada, 2016)

Una vez analizada la situación actual de la compañía se procedió a realizar el Diseño de Arquitectura de Implementación en la nube por medio del cual se migrará la información entregada para su migración, análisis y publicación de reportes.

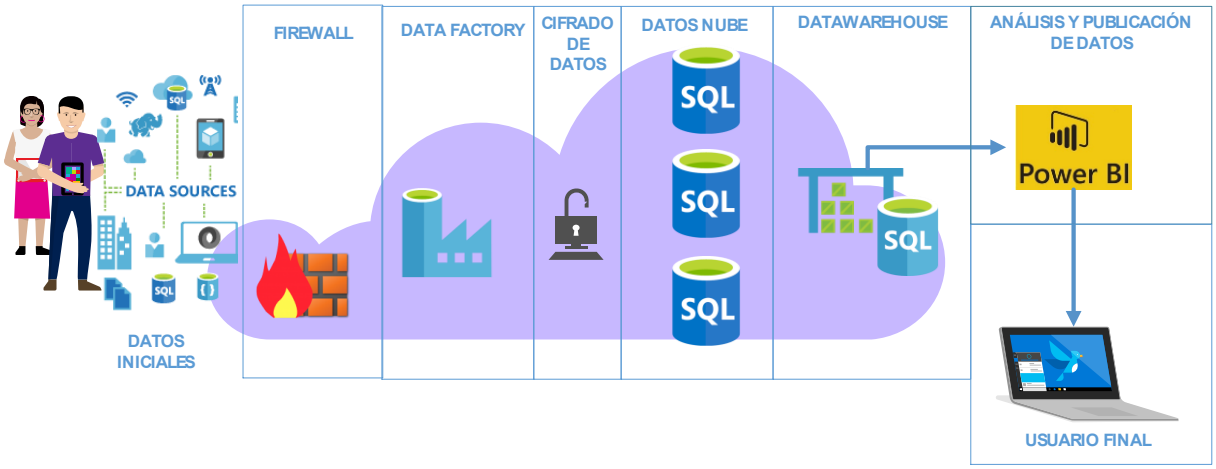


Ilustración 26: Diseño de Arquitectura de Implementación en la nube

Fuente: (Lozada, 2016)

En la ilustración la cual hace referencia al **Diseño de Arquitectura de Implementación en la nube** explica brevemente:

1. Entrega de información de la compañía localizados en diferentes fuentes locales y externas: Archivos de texto plano, documentos en Excel y base de datos implicados, todos estos archivos entregados formarán parte de la migración a la nube seleccionada.

2. Una vez analizada la información se procederá a realizar la limpieza de datos de tal manera de obtener una calidad de datos aceptable.

3. Una vez que tenemos la información preparada para la migración, se procede a configurar las instancias de manera local y en la nube.

4. En la instancia configurada en la nube se aplicará un firewall de autentificación mediante una base de datos No SQL, en donde se procederá a registrar las IP de los equipos autorizados, usuarios y contraseñas para el ingreso.

5. Antes de que la información sea transferida se procede a realizar el cifrado de datos de las bases de datos configuradas: STG, ODS y DWH. El procedimiento de cifrado deberá ser documentado.

6. Para la transferencia de información se configurará un flujo en Data Factory (herramienta propia de Microsoft Azure para transferencia de información).

7. Las bases de datos serán auditadas, por lo que se mantendrá el registro de su actividad en tiempo real en bases No SQL.

8. Se procede armar cubos de información los cuales estarán localizados en la base de datos DWH y estos procederán a ser parte del Datawarehouse.

9. A partir de Datawarehouse se presenta la información bajo la metodología, estándares y controles seleccionados; como también los reportes requeridos por medio de Power BI al usuario final.

Fase 3: Verificar

En esta fase realizaremos el diseño de proceso de implementación de tratamiento de riesgos, un esquema detallado de la arquitectura de implementación en la nube, como también el esquema detallado de la información del proceso seleccionado.

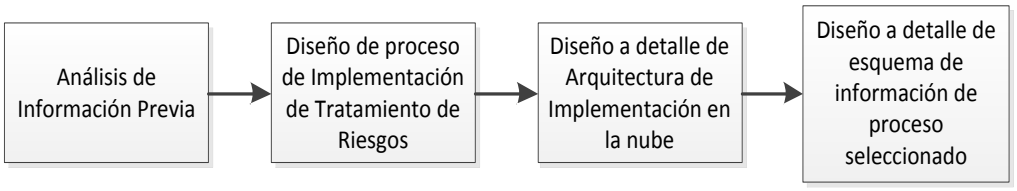


Ilustración 27: Proceso de Verificación SGSI

Fuente: (Lozada, 2016)

Fase 4: Actuar

En esta fase, se analizará y verificará que cada uno de los procesos detallados en fases anteriores se encuentre de forma correcta en la implementación final de nuestro esquema de seguridad, se documentará paso a paso la respectiva implementación como también su presentación de datos finales por medio de una demo.

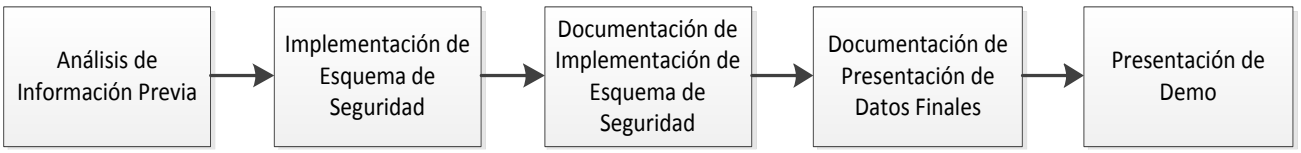


Ilustración 28: Proceso de Actuar/Final en SGSI

Fuente: (Lozada, 2016)

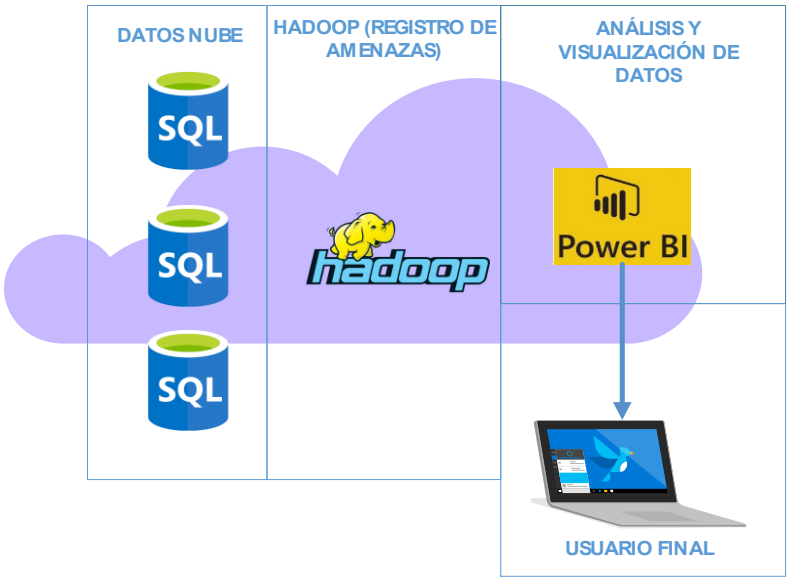


Ilustración 29: Diseño de esquema de información de proceso seleccionado

Fuente: (Lozada, 2016)

En la información de la **Ilustración 28** referente al **Diseño de esquema de información de proceso seleccionado** explica brevemente:

1. Una vez que se ha procesado la información en la nube por medio de 3 bases de datos: STG, ODS y DWH realizadas con el objetivo final en inteligencia de datos y configuradas bajo los estándares y metodología establecidos.

2. Para poder dar seguimiento de la información por medio de bases de datos de auditoría como se indica en uno de los estándares seleccionados (ISO/IEC 27001) se ha configurado una base de datos No SQL en Hadoop con el propósito de almacenar cada transacción o acción realizada tanto en la información almacenada como en el servidor, de tal manera cuando se desee realizar un análisis general poder detectar posibles amenazas y alertas en tiempo real; cada uno de los registros almacenados incluirá usuario y detalle de la acción.

3. La información menciona en el punto anterior podrá ser visualizada en por medio de reportes estándar o personalizados por medio de Power BI a demanda de los usuarios.

4.1.5 Verificar

En la Ilustración 26 referente al **Proceso de verificación en SGSI** decíamos que su flujo cumplirá 4 pasos específicos, los cuales los iremos desarrollando en este punto:

1. Análisis de información previa de las fases anteriores: Planificar y Hacer.

   Se analizó y revisó los procesos respectivos a las dos fases tales como: Definición del alcance, activos de información relevantes, análisis y evaluación de riesgos y selección de controles de los estándares ISO/IEC 27001 y ISO/IEC 27018 que se encuentran en el documento de aplicabilidad que se encuentra en la parte de **Anexos** (Anexo 1), con el propósito de mitigar los riesgos de la información de la compañía.

2. Diseño de proceso de Implementación de Tratamiento de Riesgos en la nube seleccionada. (Microsoft Azure).

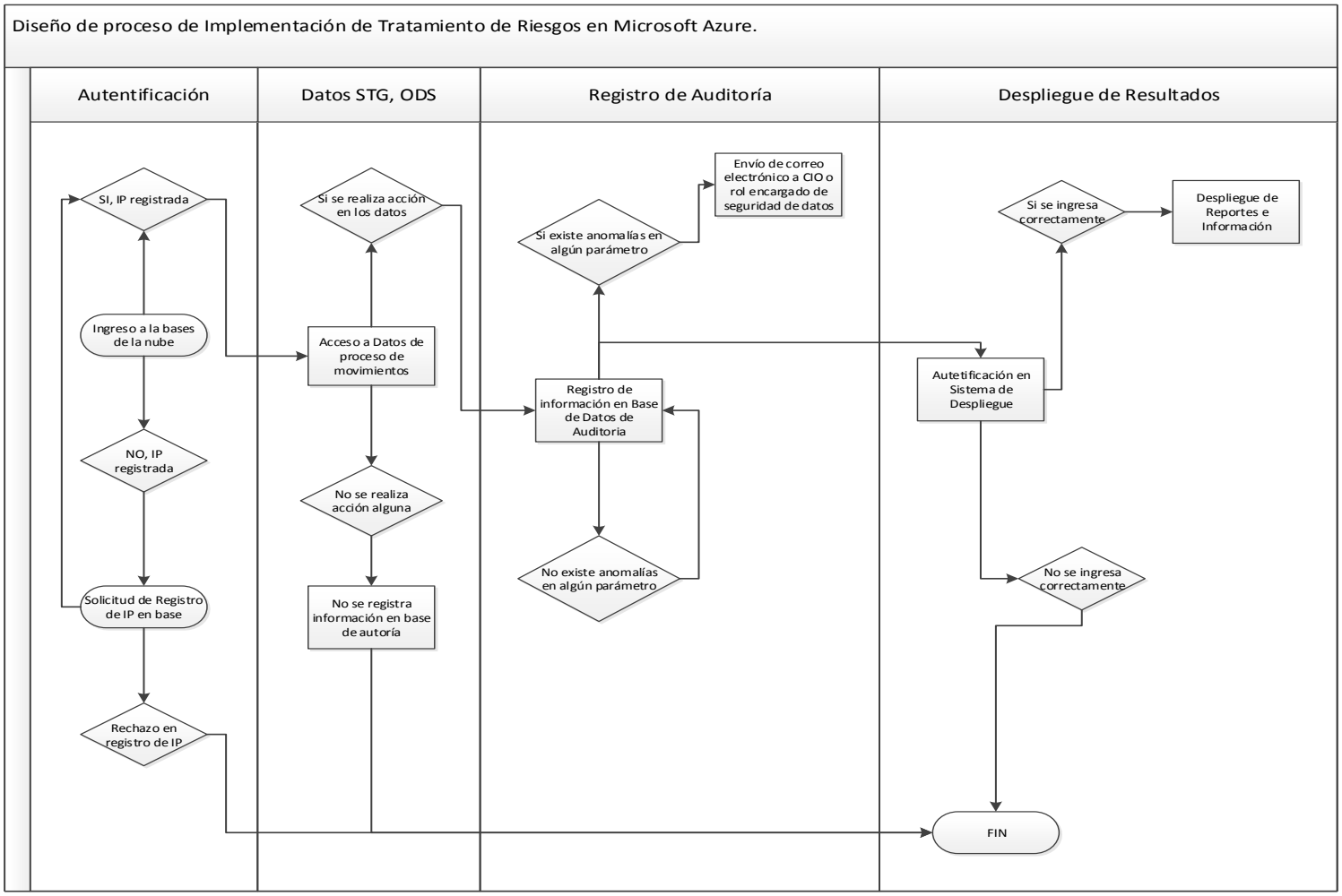


Ilustración 30: Diseño de proceso de Implementación de Tratamiento de Riesgo en Microsoft Azure

Fuente: (Lozada, 2016)

Flujo de proceso:

- **Autentificación:** Para acceder a la información a partir de SQL Server, Power BI u Azure Storage Explorer, se realizará la primera verificación dentro de los datos en donde se buscará si la IP desde donde se accede a la información se encuentra registrada, caso contrario se deberá solicitar su registro; una vez registrado y aprobado se podrá acceder a la información según la asignación de responsabilidades.

- **Datos almacenados en STG, ODS:** En este paso se refiere a las acciones realizadas en las bases de datos, si se detecta algún tipo de acción se almacenará automáticamente en la base de datos específica para la auditoría, la información almacenada puede ser: consulta, transferencia de información, ingreso a los datos desde herramientas externas, en caso de detección de amenazas o anomalías será reportado en tiempo real vía correo (correos registrados para reporte de anomalías); en caso de que no se registre anomalías o amenazas el flujo procederá a los siguiente pasos.

- **Registro de Auditoría:** El administrador o encargado de los datos será informado inmediatamente, caso contrario solo se almacenará en la base de datos de auditoría sin este paso.

- **Despliegue de Resultados:** Se procederá a solicitar las credenciales correspondientes para ingresar a los datos para poder visualizar los reportes e información almacenada a detalle, caso contrario al no tener acceso a la información finalizaría el proceso sin este paso.

3. Diseño a detalle de Arquitectura de Implementación en la nube.

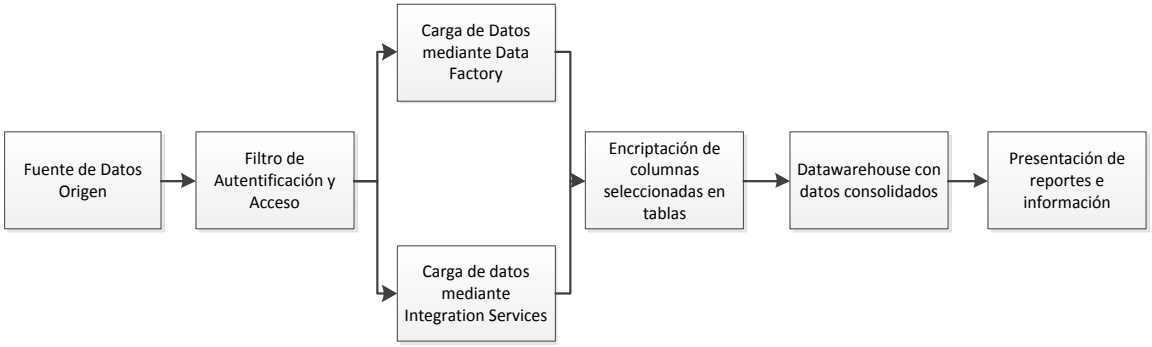


Ilustración 31: Diseño a detalle de Arquitectura de Implementación en la nube

Fuente: (Lozada, 2016)

- El cliente proveerá la información requerida para la mejora de procesos e ingresos, para ellos se solicitó base de datos que contengan movimientos y clientes en formatos txt, Excel y tablas de base de datos en SQL Server almacenadas de forma local.

- La información mencionada anteriormente se procesará mediante ETLs desarrollados de forma local y nube; utilizando SQL Server Integration Services, por medio de la nube utilizando Data Factory o por carga local mediante query colocando los datos de conexión correspondiente al servidor.

- Previo a esto se pasará por dos filtros de autentificación y acceso en cada una de las herramientas; el primero será el registro de la máquina asignada y el segundo por medio de usuario y contraseña asignado para la cuenta de almacenamiento.

- Las tablas que se encuentran en la nube son previamente creadas en una cuenta de almacenamiento, algunos de los campos o tablas son encriptados mediante queries, los cuales se encuentran en la parte de **Anexos (Anexo 2 y 3)**

- Recalcando, las bases de datos e información almacenada se encuentran configuradas bajo controles seleccionados de los estándares ISO/IEC 27001/27018.

- Se procede a transferir la información migrada a la nube de manera consolidada al SQL Datawarehouse.

- Previo al ingreso a Power BI se realizará un filtro de autentificación y acceso en la herramienta mediante usuario y contraseña de cuenta de almacenamiento, como se ha mencionado anteriormente, según las responsabilidades asignadas se podrá visualizar la información almacenada.

- Por medio de este último se realizarán los correspondientes reportes y análisis de la información.

4. Diseño a detalle de esquema de información de proceso seleccionado (Este esquema se utilizará cuando se desee actualizar la información migrada a la nube, o en el caso de que la compañía decida crear nuevas tabla o modificar reportes predeterminados).

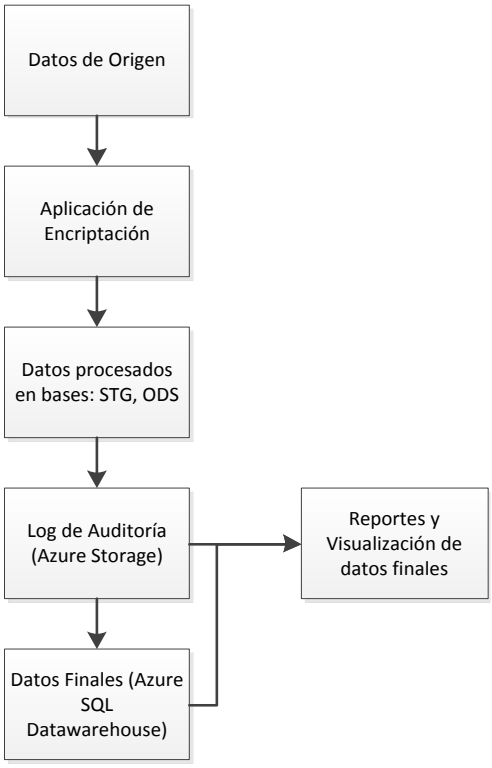


Ilustración 32: Diseño a detalle de esquema de información de proceso seleccionado

Fuente: (Lozada, 2016)

4.2 Implementación de Esquema de Seguridad

4.2.1 Actuar

En el punto **4.1.4 Hacer** en la **Ilustración 27** referente al **Proceso de actuar en SGSI** podemos observar que se encarga de 5 pasos específicos, los cuales los desarrollaremos en este punto, estos son:

1. **Análisis de Información Previa Desarrollada:** En este punto se analizó las tres fases previamente determinadas para que se lleve una implementación de acuerdo a lo diseñado paso a paso.

2. **Implementación de Esquema de Seguridad en la nube:** Se llevó acabo toda la implementación tal como indicamos en un principio en la arquitectura

determinada sin cambio alguno tal como podemos revisar en **Ilustración 16** e **Ilustración 17** de manera detallada.

3. Documentación de Implementación de Esquema de Seguridad, en este punto detallaremos lo implementado, lo cual se visualizará a detalle en la **Ilustración 32**:

    - Se procedió a crear una estructura de 2 bases de datos en Azure SQL Database y 1 base final en Azure SQL Datawarehouse, backups de seguridad, múltiples bases de datos No SQL para el registro de actividades para detección de amenazas en tiempo real.

    - En la primera base denominada STG que se encuentra alojada la información de tarjetas de crédito, movimientos y cuentas representativas de sobregiro.

    - En la segunda base denominada ODS, de la información alojada en el STG se realizó varias tablas para el análisis de información con el fin de búsqueda de iniciativas para mejora de procesos e ingresos de la compañía.

    - Y por último en la base denominada DWH se encuentra la información para los reportes a demanda.

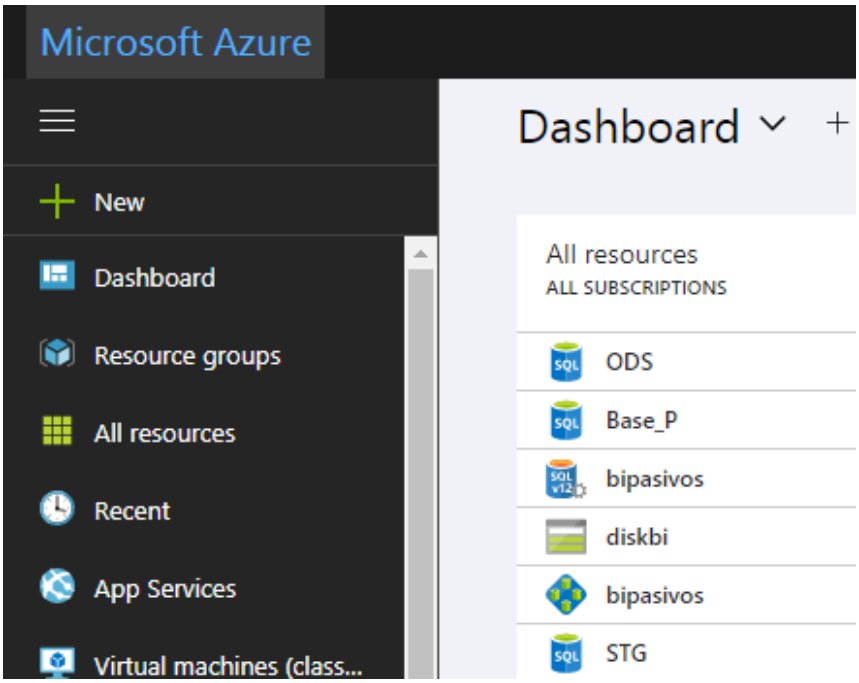


Ilustración 33: Dashboard en Microsoft Azure

Fuente: (Lozada, 2016)

En el Dashboard en Microsoft Azure, permite visualizar nuestras instancias creadas como son: Base de datos SQL o No SQL (para el almacenamiento de logs de transacciones y auditorias) de nuestro esquema de seguridad propuesto.

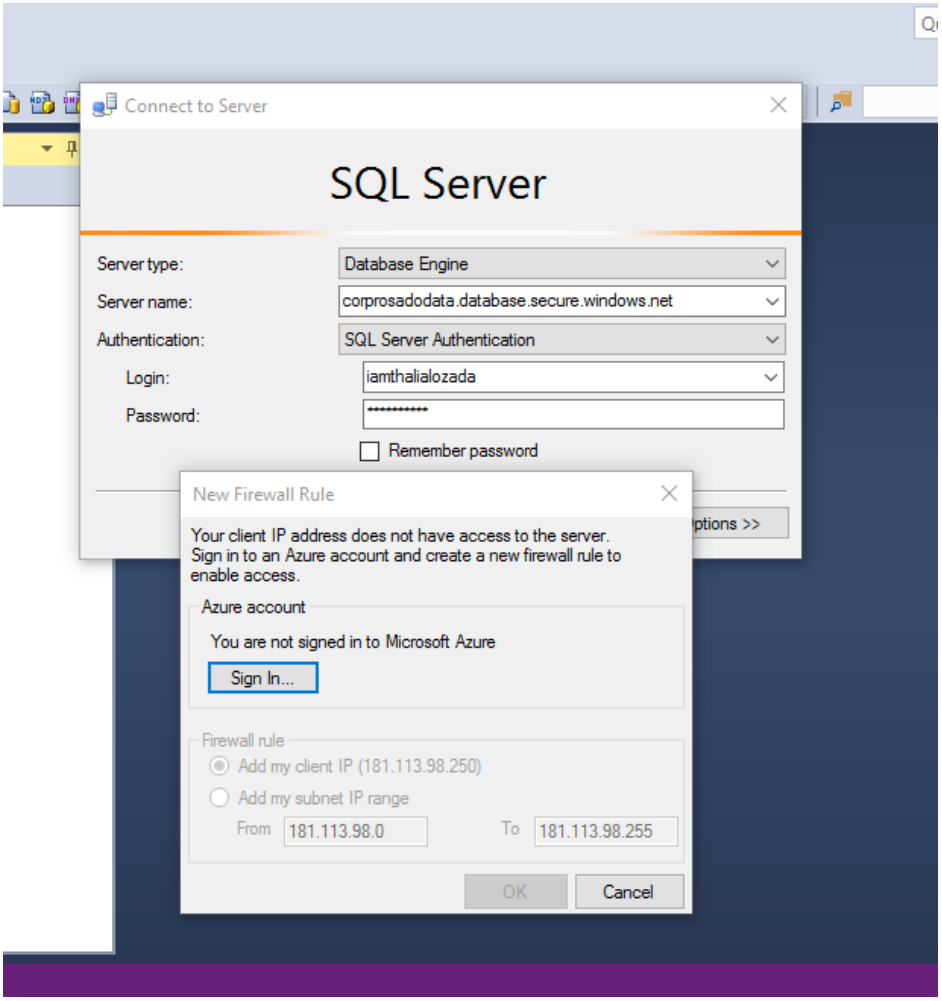


Ilustración 34: Autentificación y acceso SQL Azure (sin registro previo de IP)

Fuente: (Lozada, 2016)

Por medio de la herramienta SQL Server 2014, podremos acceder a las bases de datos migradas a la nube bajo un esquema de seguridad, se lo realiza mediante esta herramienta para visualizar la información, establecer reportes, niveles de seguridad, entre otros.

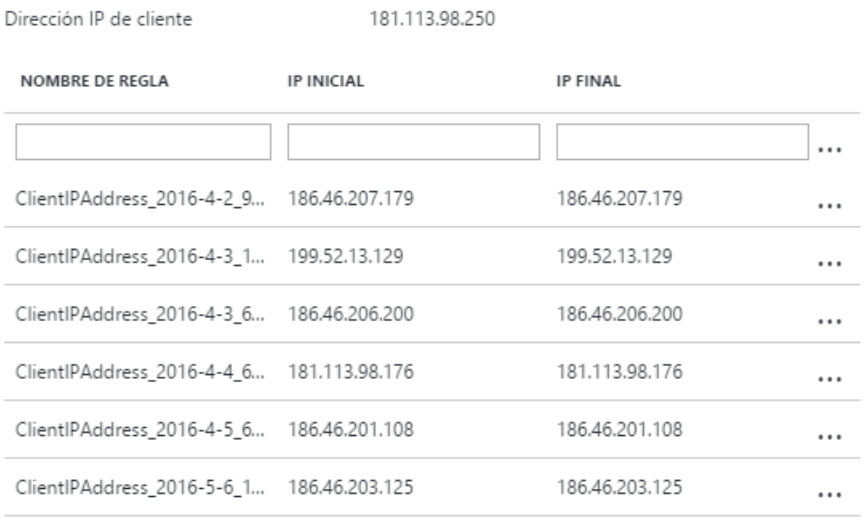


Ilustración 35: Registros de Clientes IP para acceso autorizado

Para que cualquier usuario pueda acceder a la información de las bases, la IP de la máquina debe ser ingresada en la base de datos, esto es almacenado en una tabla dedicada para ello.

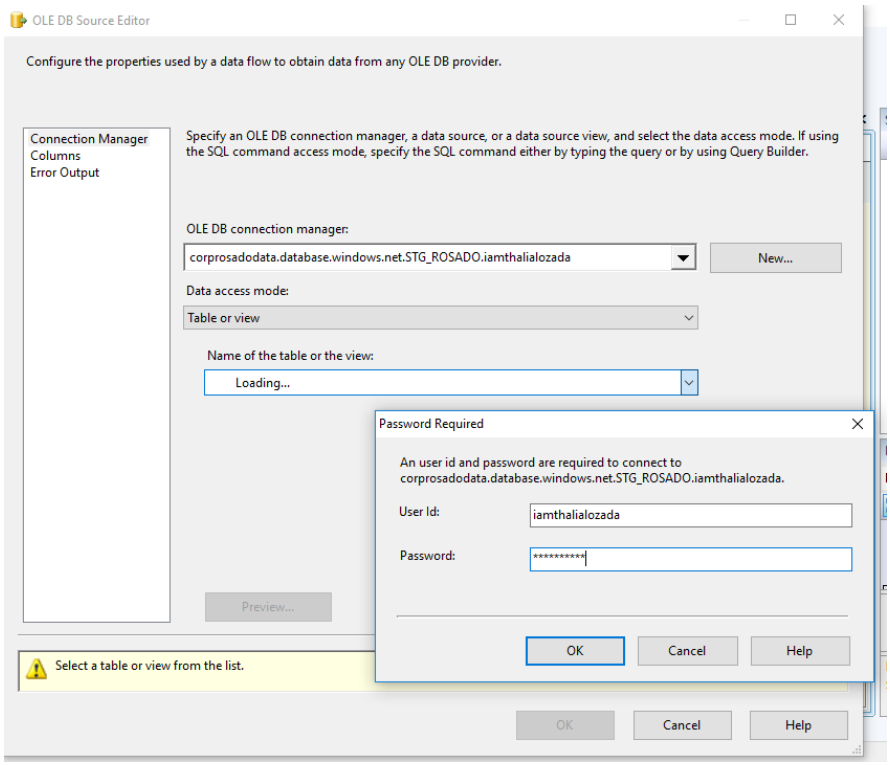


Ilustración 36: Autentificación y registro de acceso a Visual Studio Business Intelligence

Fuente: (Lozada, 2016)

Por medio de la autentificación, se verifica y otorga los permisos según las actividades del usuario, accediendo a las bases de datos determinadas para la migración. Cuando se requiera alguna información específica se desplegará mensajes de ayuda.

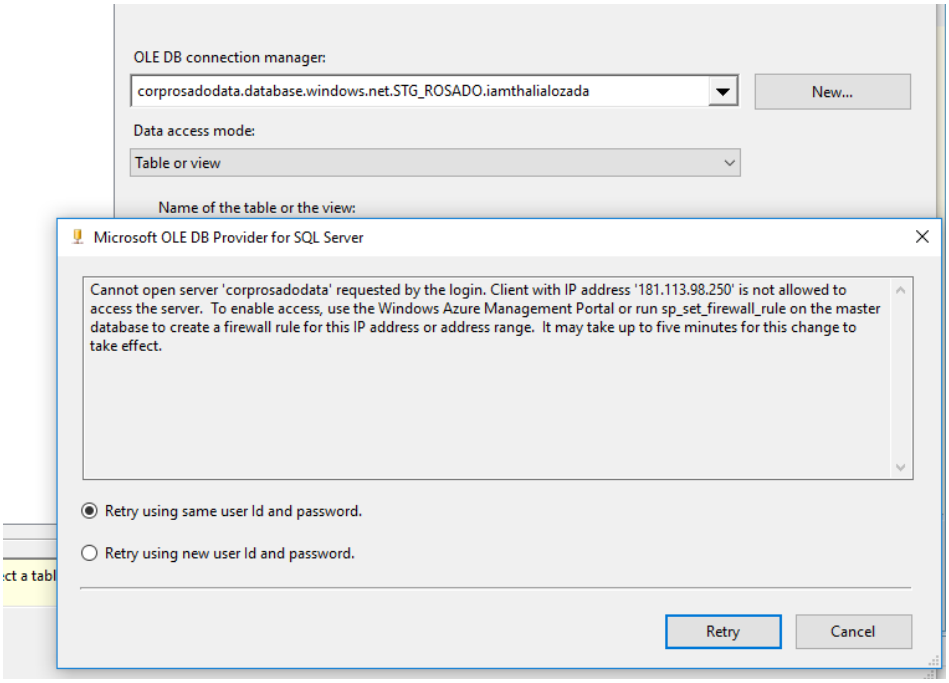


Ilustración 37: Acceso no registrado en la base de datos de IPs en el caso de la herramienta Visual Studio Business Intelligence

Fuente: (Lozada, 2016)

Como se menciona en diagrama de proceso en la **Ilustración 29** al momento que se busca que la IP registrada, caso contrario se obtendrá un mensaje de que el acceso no está permitido.

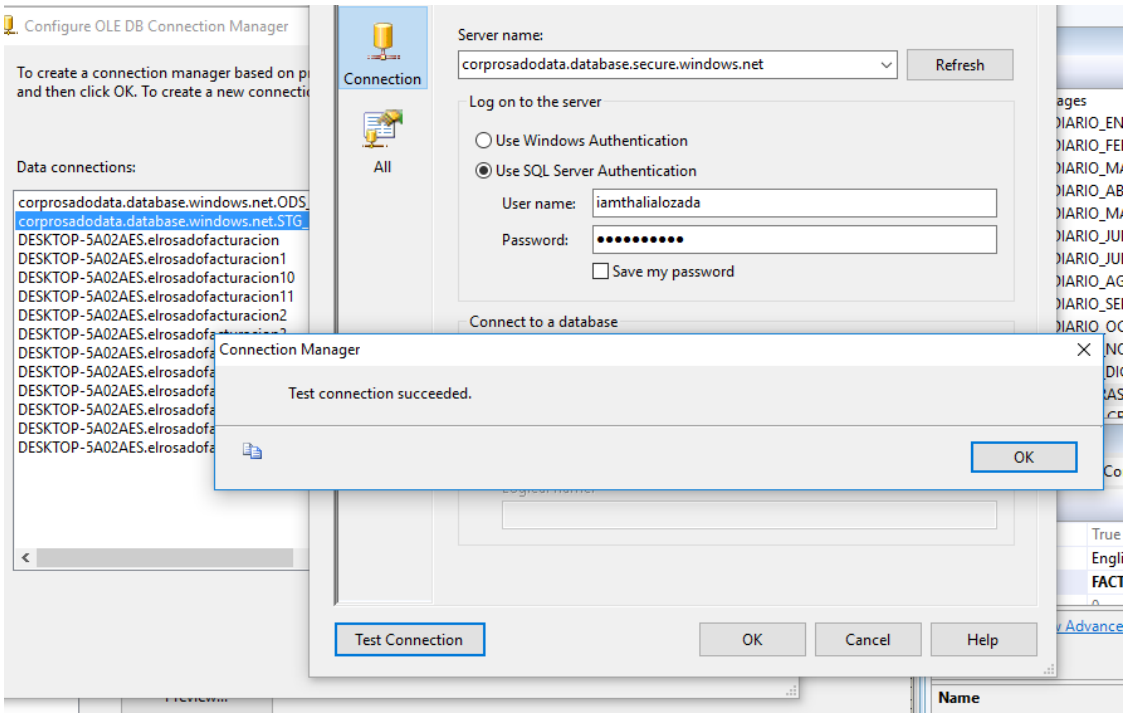


Ilustración 38: Test de conexión a bases de datos en la nube para proceso ETL

Fuente: (Lozada, 2016)

Una vez que se ha registrado la IP asignada, y es asignado su usuario y contraseña dependiendo de las actividades asignadas en la migración; se obtendrá una conexión exitosa.

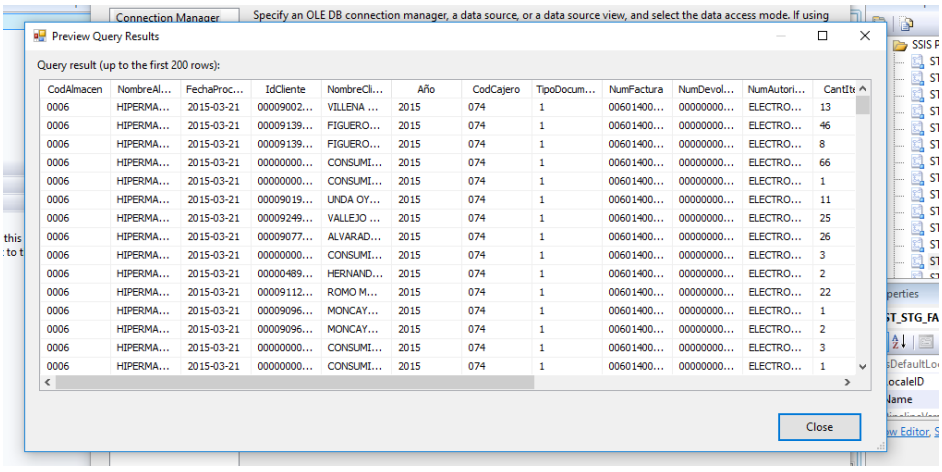


Ilustración 39: Pre visualización de información en carga ETL

Fuente: (Lozada, 2016)

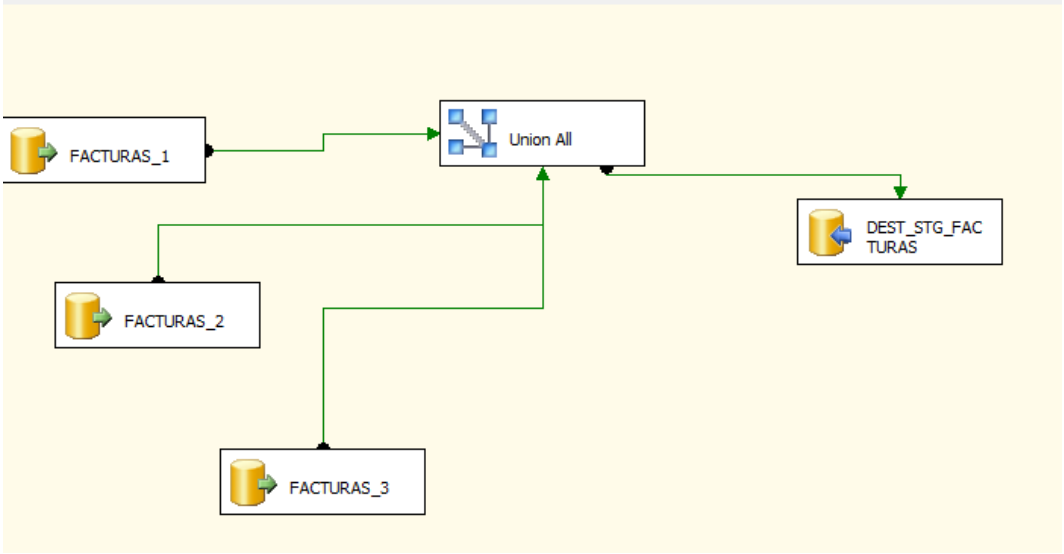


Ilustración 40: Diseño de Carga ETL

Fuente: (Lozada, 2016)

La información seleccionada para la migración mantiene la estructura de origen y la misma fue entregada en documentos planos, Excel, entre otros, la cual fue colocada en distintas bases locales.

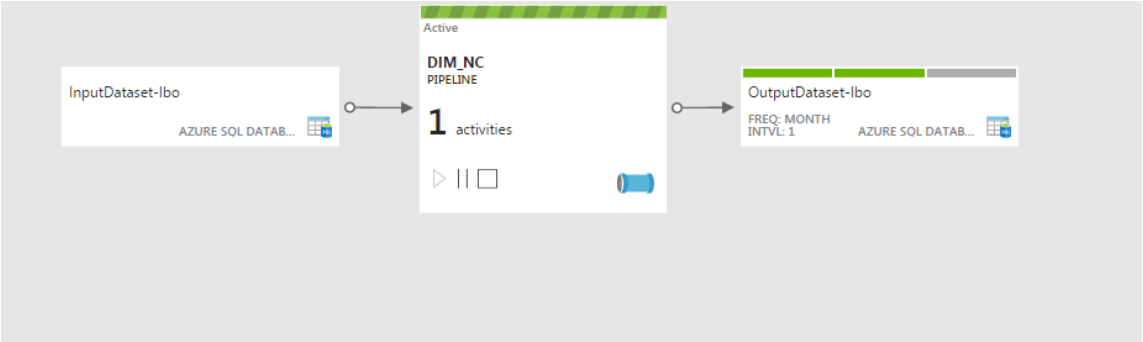


Ilustración 41: Proceso ETL desarrollado en Data Factory para carga de datos en ODS

Fuente: (Lozada, 2016)

Después que la base de datos STG es cargada con la información se procede a utilizar Data Factory (herramienta de ETL en Microsoft Azure) para la carga de base de datos ODS

Luego se procede hacer un consolidado de datos en Azure SQL Datawarehouse, para presentar los reportes al usuario final.

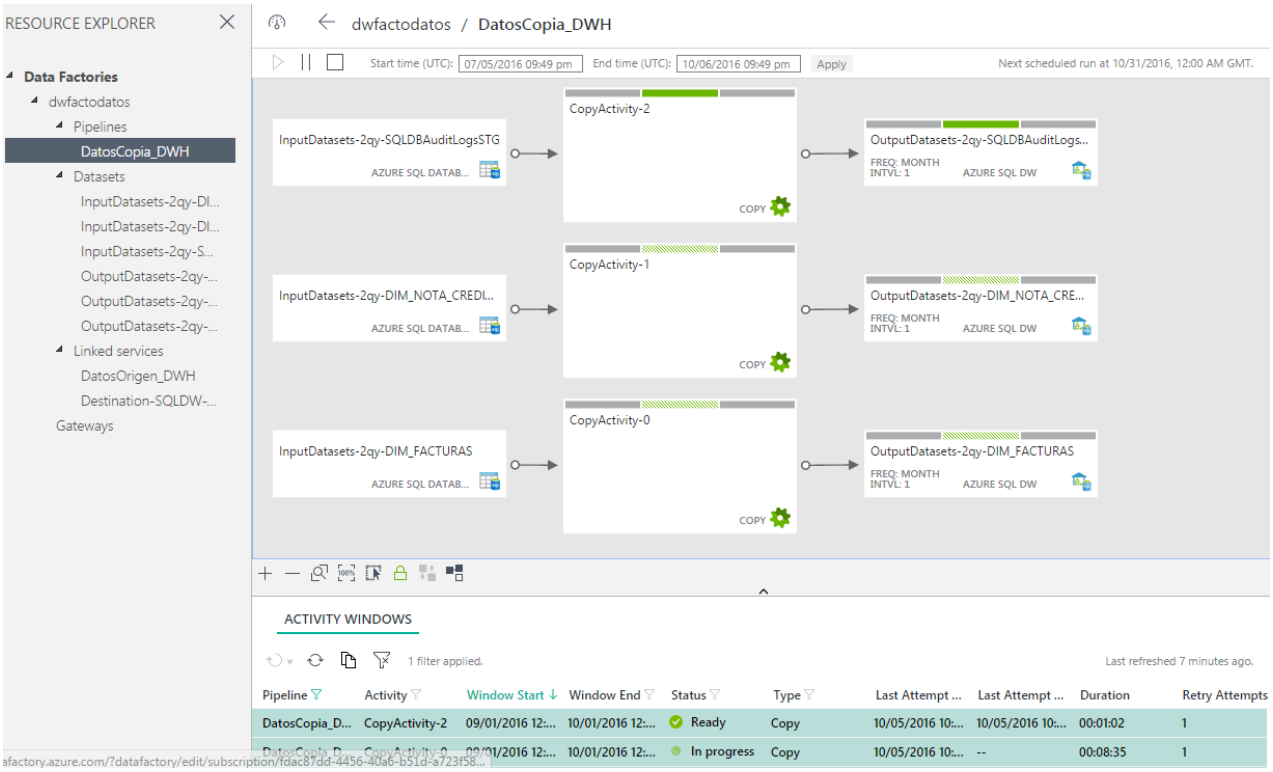


Ilustración 42: Carga de Datos de Datawarehouse por medio de ETL en Data Factory

Fuente: (Lozada, 2016)

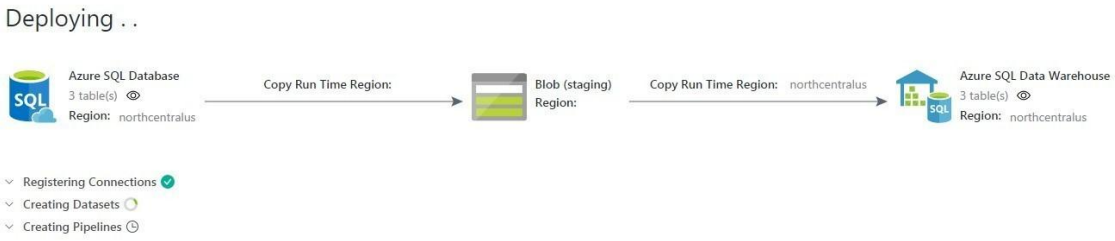


Ilustración 43: Despliegue de datos en Datawarehouse utilizando Data Factory

Fuente: (Lozada, 2016)

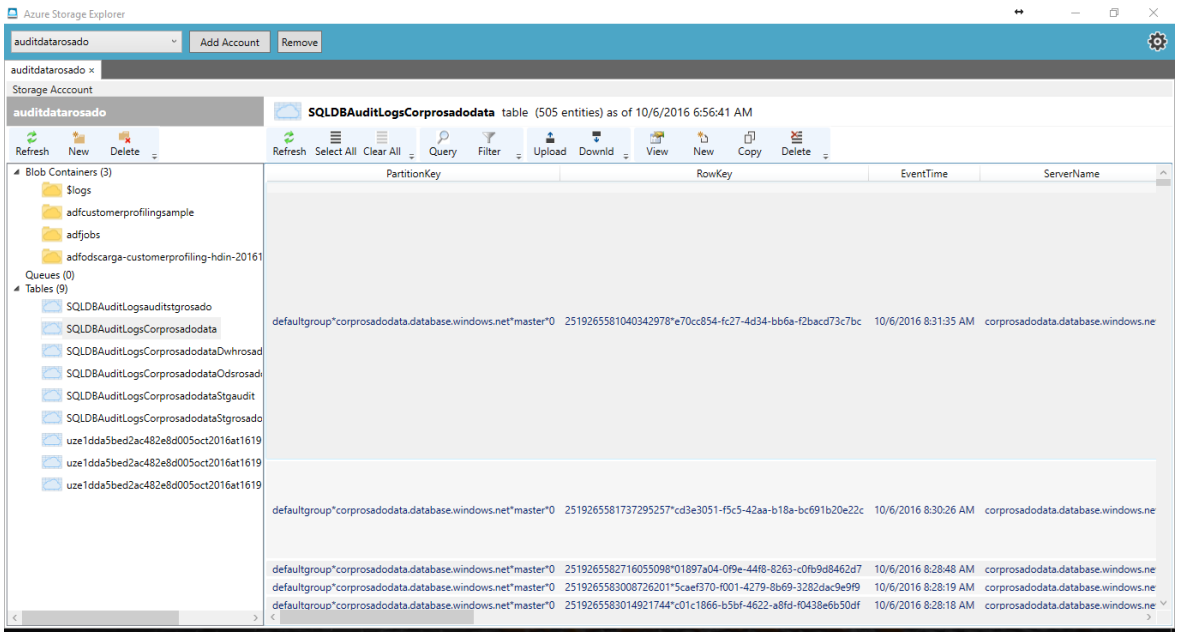


Ilustración 44: Visualización de Audit Logs en Azure Storage Explorer

Fuente: (Lozada, 2016)

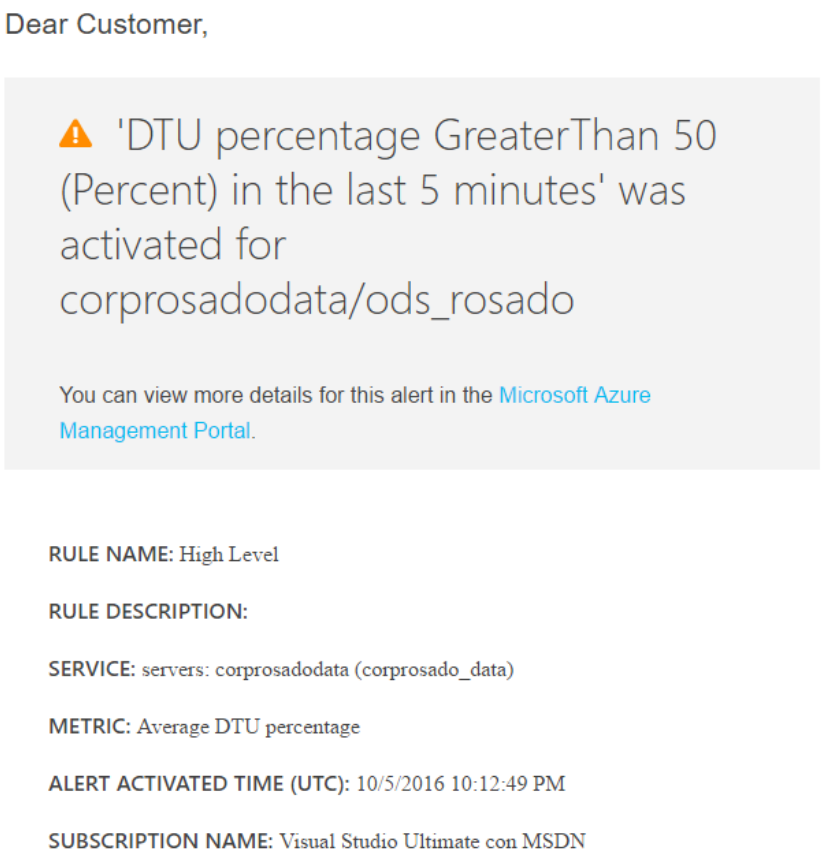


Ilustración 45: Correo de alertas para detección de amenazas

Fuente: (Lozada, 2016)

4. El cifrado es el proceso consistente en alterar los datos mediante el uso de una clave o contraseña, el cual proviene de años atrás. Los primeros sistemas de cifrado se vinculaban con los militares con la necesidad de evitar que los enemigos conocieran acerca de los movimientos de las tropas al interceptar mensajes.

5. En el **Anexo 2** se podrá encontrar el código criptográfico desarrollado para la información sensible entregada para el desarrollo del esquema de seguridad.
   La **ilustración 45** muestra que cada nivel de la jerarquía de cifrado cifra el nivel que tiene por debajo, además muestra las configuraciones de cifrado más comunes. El acceso al principio de la jerarquía se suele proteger mediante una contraseña.

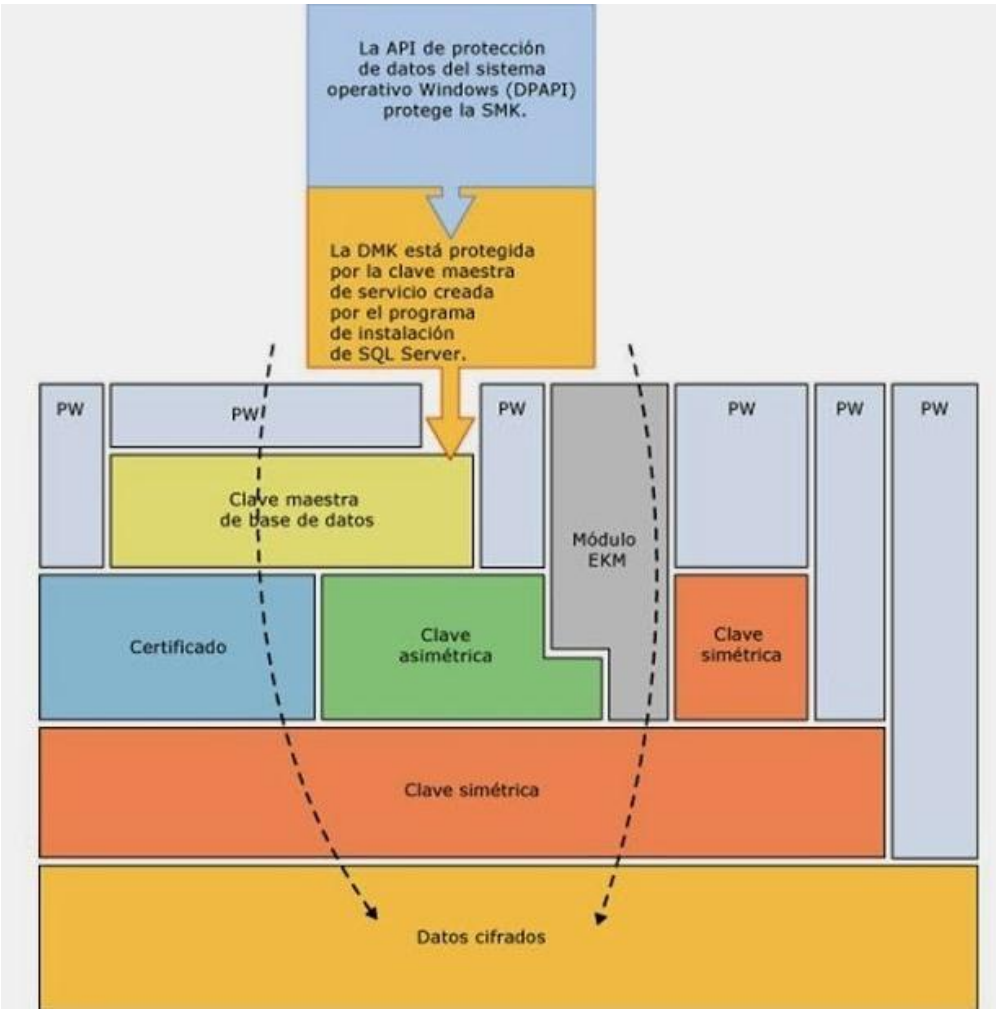


Ilustración 46: Jerarquía de cifrado de datos

(Microsoft , 2016)

4.3 Muestra de reportes finales del proceso seleccionado

1. Documentación de Presentación de Datos Finales

Se realizaron varios reportes y presentación de datos según las necesidades del negocio generados en Excel y Power BI, algunos de ellos presentados a continuación:

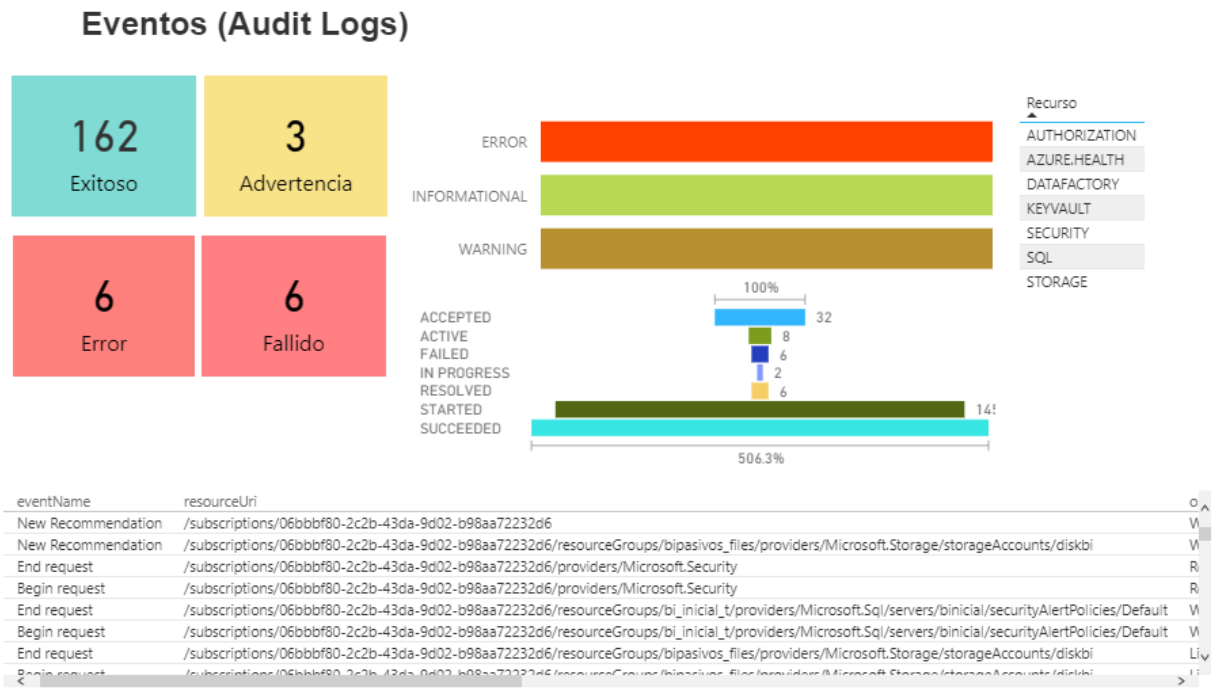


Ilustración 47: Reporte de Logs almacenados en Hadoop por cada base de datos migrada

En el reporte presentado en la **Ilustración 46**, podemos visualizar los eventos registrados por cada una de nuestras bases en Hadoop, de manera consolidada utilizando los campos correspondientes al recurso, eventos, tipo y acción realizada.

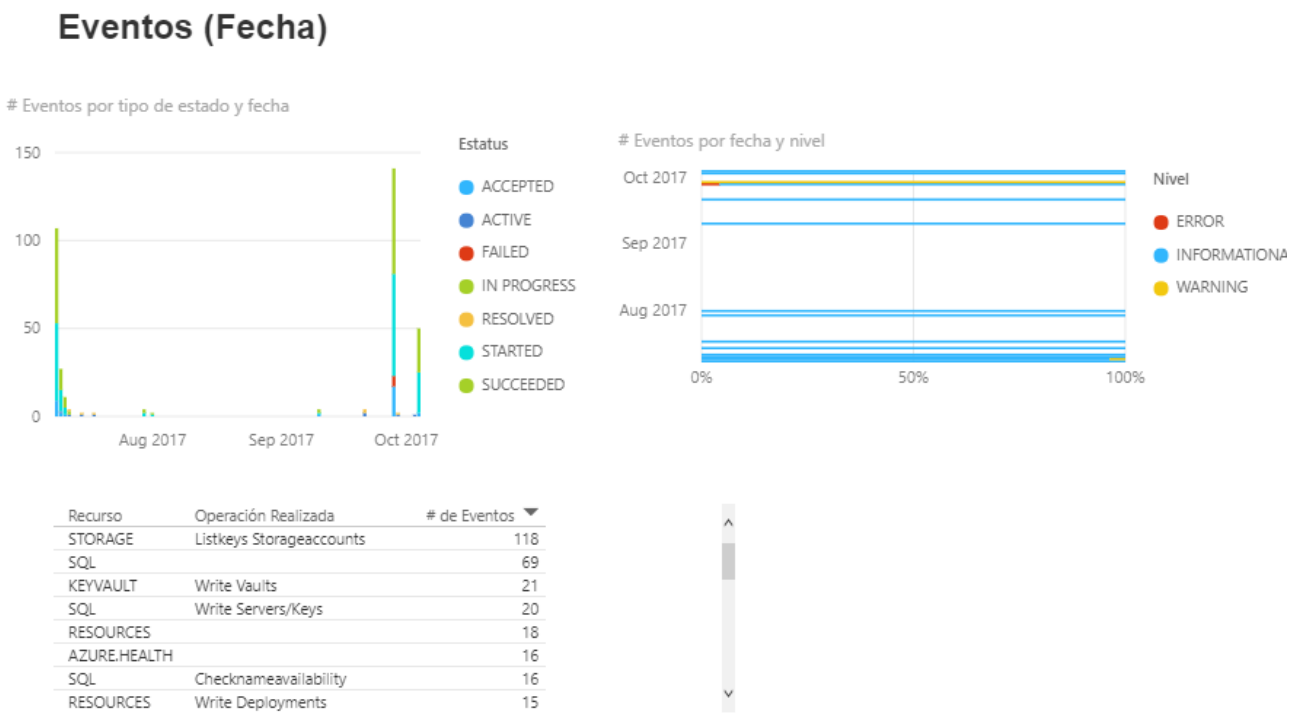


Ilustración 48: Reporte de Logs almacenados en Hadoop por cada base de datos migrada en base a la fecha

En el reporte presentado en la **Ilustración 47**, podemos visualizar los eventos registrados por cada una de nuestras bases en Hadoop, de manera consolidada utilizando los campos correspondientes al recurso, número de eventos, tipo y acción realizada por meses; y fechas específicas.



Ilustración 49: Reportes orientados a la información entregada por la compañía

En el reporte presentado en la **Ilustración 48**, es parte de los generados para encontrar iniciativas de mejora de ingresos para la compañía, en esta iniciativa podemos visualizar que la comisión asociada a un cheque en cámara de compensación no se lo está cobrando de la manera adecuado, ni empleando las mejores prácticas.

Capítulo V: Conclusiones y recomendaciones

5.1 Conclusiones

Una vez finalizado el caso de estudio y haber realizado el respectivo análisis, evaluaciones, diseños e implementación demostrativa del esquema de seguridad utilizando Microsoft Azure, se concluye que:

1. La implementación de un Sistema de Gestión de Seguridad de la Información dentro de las compañías basado en normas o estándares para administrar el control de seguridad de la información, procesos y procedimientos de forma documentada ayudan a mantener un gobierno de TI centralizado, agregando valor al personal involucrado y su directiva.

2. Es de gran importancia establecer el objetivo principal y alcance al implementar un esquema de seguridad utilizando metodologías, para poder adecuar a las necesidades y riesgos actuales de la compañía.

3. Además de detectar las necesidades y riesgos de la compañía como adicional si la compañía cuenta con procesos de seguridad de la información como buena práctica según la ISO/IEC 27001 es necesario auditarlos para mantener una idea clara de cómo el personal los encuentra aplicando y cumpliendo los controles previamente establecidos para reforzar mejoras.

4. Se mantiene un nivel de seguridad intermedio para protección de la información de la compañía visualizada en el análisis según las metodologías empleadas ISO/IEC 27001, pero se detectó muy fácilmente que no mantiene un plan de respaldos de la misma, indicaron que solo mantienen históricos en producción de los últimos seis meses. La información antes del tiempo indicado podría encontrarse incompleta, reduciendo posibilidades de mejora de ingresos.

5. La mejor práctica de gestión de seguridad de la información para que la implementación pueda funcionar de la mejor manera, debe formar parte de la cultura organizacional de las compañías ecuatorianas; y en cada una de ellas la implementación de un sistema de gestión logrará cumplir mejor las expectativas con el apoyo de la alta gerencia como promotor activo de la seguridad de la información en la empresa.

6. A pesar que se implemente un SGSI exitoso, el mismo debe ser actualizado en un periodo de tiempo preestablecido. Esto se lo realiza porque con el tiempo se presentan más activos de información, nuevos tipos de amenazas, vulnerabilidades y riesgos; por las razones antes mencionadas la empresa debe estar preparada para poder actuar de forma inmediata ante nuevas amenazas que sean identificadas en las actualizaciones.

7. Con la información entregada y en la manera que se la encontró los empleados no trabajan bajo una manera adecuada, muchos empleados tienen a documentar todo y otros creen que la documentación de los procesos es una pérdida de tiempo; pero la realidad de la documentación de los procesos es que la deben tomar en cuenta como una herramienta de importancia para el mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información (SGSI).

5.2 Recomendaciones

1. Se recomienda una capacitación de forma constante o periódica a todo el personal indicando las políticas, procedimiento, procesos, estándares para manejo de información, para evitar inconvenientes de amenazas o vulnerabilidades por parte de usuarios a futuro.

2. Como una mejor práctica y con el fin de evitar riesgos evidentes como son: fraude, robo, manipulación, modificación de la información, la misma debe ser clasificada por tipos: confidencial y exclusiva para ciertos roles de usuarios, crítica, sensible, libre acceso y pública.

3. Se recomienda que durante el ciclo PCDA del SGSI, la empresa debería tener la mayor información posible al momento de aplicar los criterios y lineamientos corporativos para la estimación de riesgos, permitiendo escalar riesgos locales percibidos, alinear los planes de gestión de la seguridad de la información de la mejor manera, en función de los recursos, objetivos y condicionantes.

4. Se recomienda aplicar esfuerzos para cumplir con la implementación de manera exitosa, ya que el diseño que permite asegurar la gestión de la seguridad de la información ha sido realizado bajo la norma ISO/IEC 27001, la compañía es certificable.

5. Luego de la implementación de los primeros procesos y activos de información seleccionados, se puede realizar diseños similares para los demás procesos de la empresa. De igual manera elaborar un plan de continuidad de negocio, por medio de esto se reforzará la seguridad de la empresa y además diseñar un plan de auditoría periódica para analizar la variación de los niveles de seguridad de la empresa en el tiempo.

6. Se recomienda establecer mecanismos o estrategia que permitan identificar nuevos activos de información para la toma de decisiones a tiempo frente a nuevas vulnerabilidades, amenazas o riesgos detectados; y en base a la información tomar acciones preventivas.

7. Es recomendable documentar los procesos para poder administrarlos de manera óptima y hacer frente a cualquier cambio dentro de la empresa. La documentación de procesos también permite la mejora de los mismos.

Bibliografía

- DELL. (2015). Global Technology Adoption Index 2015. 2016, de DELL Sitio web: http://en.community.dell.com/dell-blogs/direct2dell/b/direct2dell/archive/2015/10/08/global-technology-adoption-index-2015
- David Mitchell Smith. (Abril 2016). Cloud Computing Primer for 2016. Gartner, 1, 12. 2016
- David López Jiménez. (2013). Cloud Computing Analyzed From the Spanish Legal System. 2016, de Revista de derecho (Valparaíso) Sitio web: http://www.scielo.cl/scielo.php?pid=S0718-68512013000100021&script=sci_arttext
- Rackspace Hosting. (2011). The Cloud Computing Stack. UNDERSTANDING The Cloud Computing Stack SaaS, Paas, IaaS (17). US
- Joshy Joseph. (2009). Cloud Computing - Patterns For High Availability, Scalability, And Computing Power With Microsoft Azure. 2017, de MSDN Sitio web: https://msdn.microsoft.com/en-us/magazine/dd727504.aspx
- David W. Cearley. (2010). Cloud Computing, Key Initiative Overview, Gartner.
- ONTSI (Observatorio Nacional de las Telecomunicaciones y de la SI). (2012). Cloud Computing, Retos y Oportunidades. España: Gobierno de España.
- Microsoft. (2016). What is cloud computing? 2016, de Microsoft Sitio web: https://www.microsoft.com/en-us/server-cloud/solutions/cloud-computing.aspx
- IDC (2013), "IDC Forecasts Worldwide Public IT Cloud Services Spending to Reach Nearly $108 Billion by 2017 as Focus Shifts from Savings to Innovation", http://www.idc.com/getdoc.jsp?containerId=prUS24298013.
- HP Ecuador. (2016). Servicios Cloud Computing, HP Ecuador. 2016, de HP Sitio web: https://www.hpe.com/lamerica/es/services.html
- LOL Cloud. (2016). Información de Costos de Nube. 2016, de Licencia Online Sitio web: http://www.licenciasonline.com/ec/es/cloudhttps://www.hpe.com/lamerica/es/services.html
- Claro Ecuador. (2016). Servicios Cloud. 2016, de Claro EC Sitio web: www.clarocloud.com.ec/
- Computerworld. (2015). Cloud. Computerworld, 268
- Rackspace. (2016). Dedicated Hosting Solutions 2016, de Rackspace Sitio web: https://www.rackspace.com/managed-hosting
- IDC. (2016). CloudView 2016: The Rapid Embracement of Cloud . 2016, de IDC Sitio web: http://www.idc.com/getdoc.jsp?containerId=US41636616
- Frost & Sullivan. (2015). 5 principios de Adopción en la Nube. 2016, de Coursehero Sitio web: https://www.coursehero.com/file/pglmvu/Frost-Sullivan-ha-identificado-5-principios-b%C3%A1sicos-para-la-adopci%C3%B3n-de/

- Uma Avantsa. (2011). Limitations of Cloud Computing. 2016, de Meghainfotech Sitio web: https://meghainfotech.wordpress.com/2011/04/21/limitations-of-cloud-computing/
- Microsoft. (2016). Código de conducta para proteger los datos personales en la nube: ISO/IEC 27018. 2017, de Microsoft Sitio web: https://www.microsoft.com/es-xl/TrustCenter/Compliance/ISO-IEC-27018
- Varios. (Febrero 2015). ISO 27018. ISOfocus en el cloud, 52.
- Dejan Kosutic. (2016). ISO 27001:2013 FOUNDATIONS COURSE. 2016, de Advisera Sitio web: https://training.advisera.com/course/iso-27001-foundations-course/
- Microsoft Trust Center. (2015). ISO/IEC 27001. Abril, 2016, de Microsoft Sitio web: https://www.microsoft.com/en-us/TrustCenter/Compliance/ISO-IEC-27001
- CDSA. (2013). Content Delivery & Security Association Anti-Piracy & Compliance Programs CPS Certification Program Overview. Abril 2016, de CDSA Sitio web: http://www.cdsaonline.org/wp-content/uploads/2013/05/CDSA-Content-Protection-Security-Standard-Overview.pdf
- Alex Hsiung. (2017). A Management System for the Cloud – Why Your Organization Should Consider ISO 27018. 2017, de CSA Sitio web: https://blog.cloudsecurityalliance.org/2017/05/22/management-system-cloud-organization-consider-iso-27018/
- Rishabh Software. (2013). Cloud Security (Concerns & Planning). 2016, de Rishabh Software Sitio web: https://infographiclist.files.wordpress.com/2013/10/cloud-security-concerns-planning_51e5282f38682.jpg
- Mariana Medina. (2012). Política organizacional. Concepto y esquema en la empresa. 2017, de Gestiopolis Sitio web: https://www.gestiopolis.com/politica-organizacional-concepto-y-esquema-en-la-empresa/
- Paul van Kessel, Jay Layman, Jonathan Blackmore, Iain Burnet, Yoshihiro Azuma. (2014). Building trust in the cloud. US: EY.
- Olga Koshelkova, Jess Martin, Guy Wanger, Dave Padmos, Jeff Liu, Channing Flynn, Pat Hyek. (2015). Cloud taxation issues and impacts. US: EY.
- Symantec. (2015). Glosario de Seguridad. 2016, de Symantec Sitio web: www.symantec.com/es/mx/theme.jsp?themeid=glosario-de-seguridad
- Vulnerabilidades. 2016, de Red y Seguridad Sitio web: http://redyseguridad.fi-p.unam.mx/proyectos/buenaspracticas/vulnerabilidades.html
- NA. (2010). La escítala. 2016, de URG Sitio web: http://www.ugr.es/~anillos/textos/pdf/2010/EXPO-1.Criptografia/02a22.htm
- By. (2017). ¿Qué son los algoritmos de encriptación AES y 3DES? 2017, de By Sitio web: https://www.by.com.es/blog/algoritmos-encriptacion-aes-3des/
- Devnull. (2016). Algoritmos de Cifrado I. 2016, de El binario Sitio web: https://elbinario.net/2016/04/05/algoritmos-de-cifrado-i/

- Wikipedia. (2017). Diffie-Hellman. 2017, de Wikipedia Sitio web: https://es.wikipedia.org/wiki/Diffie-Hellman#Descripci.C3.B3n_detallada
- Alex Hsiung, Senior Associate, Schellman & Co. (2017). A Management System for the Cloud – Why Your Organization Should Consider ISO 27018. 2017, de Cloud Security Alliance Sitio web: https://blog.cloudsecurityalliance.org/2017/05/22/managementsystemcloudorganizationconsideriso27018/

Anexos

Anexo 1:
Controles de Seguridad seleccionados para la implementación de un Sistema de Gestión de Seguridad de la Información, utilizando los dos estándares seleccionados: ISO/IEC 27001 e ISO/IEC 27018

Activo de Información	Objetivo de Control 27018	Objetivo de Control 27001	Control	Justificación
Movimientos como documento	**A.2.2**			Nube pública PII procesador de uso comercial
	A.4.1			Borrado seguro de archivos temporales
	A.9.1			Notificación de una violación de datos que implica PII
	A.9.3			PII retorno, transferencia y disposición
	A.10.6			El cifrado de información de identificación personal transmitida a través de redes de transmisión de datos públicos
	A.10.9			Registros de usuarios autorizados
		A 5.1	**A 5.1.1**	Un conjunto de políticas de seguridad de la

			información se definirá, este será aprobado por un flujo de autorización, publicado y comunicado a los empleados y partes externas relevantes.
	A.6.1	**A.6.1.1**	Todas las responsabilidades de seguridad de la información deben estar definidos y asignados.
		A.6.1.2	Las funciones en conflicto y áreas de responsabilidad deben estar separados de reducir las oportunidades de modificación no autorizada o no intencional o el mal uso de los activos de la organización.
	A.6.2	**A.6.2.1**	Una política de apoyo y medidas de seguridad que se adoptarán gestionar los riesgos introducidos mediante el uso de dispositivos móviles.
	A.7.2	**A.7.2.1**	Se deberá exigir que todos los empleados y contratistas para aplicar seguridad de

			la información de acuerdo con las políticas establecidas y procedimientos de la organización.
		A.7.2.2	Todos los empleados de la organización y, en su caso, los contratistas deberán recibir educación adecuada y la formación de la conciencia y actualizaciones regulares en las políticas y procedimientos de la organización, como relevante para su función de trabajo.
		A.7.2.3	Habrá un proceso disciplinario formal y comunicado en lugar de tomar medidas contra los empleados que han cometido una violación de la seguridad de la información.
	A.8.1	**A.8.1.1**	Activos asociados con el procesamiento de la información y las instalaciones deberán ser identificadas y

			contar con un registro actualizado.
		A.8.1.3	Reglas para el uso aceptable de la información y de los activos asociados con la información y procesamiento de información de las instalaciones deberán estar identificado, documentado e implementado.
	A.8.2	**A.8.2.1**	La información se clasificará en función de los requisitos legales, valor, criticidad y sensibilidad a la divulgación no autorizada o modificación.
		A.8.2.2	Un conjunto apropiado de procedimientos para el etiquetado de información será desarrollado e implementado de acuerdo con la información esquema de clasificación adoptado por la organización.
	A.9.1	**A.9.1.1**	Se establecerá una política de control

			de acceso, documentado y analizará con base en los requisitos de seguridad y de información de negocio.
		A.9.1.2	Los usuarios sólo deberán disponer de acceso a la red y de la red los servicios que han sido específicamente autorizados para su uso.
	A.9.2	**A.9.2.1**	Un proceso de registro de usuarios y de registro formal será implementado para permitir la asignación de derechos de acceso.
		A.9.2.2	Un proceso de provisión de acceso de usuario oficial se llevará a cabo a asignar o revocar los derechos de acceso para todos los tipos de usuario a todos los sistemas y servicios.
		A.9.2.3	La asignación y utilización de los derechos de acceso preferentemente deberá ser

			restringido y controlado.
		A.9.2.4	La asignación de la información secreta de autenticación deberá ser controlada a través de un proceso de gestión formal.
		A.9.2.5	Los propietarios de activos deberán revisar los derechos de acceso de los usuarios a intervalos regulares
		A.9.2.6	Los derechos de acceso de todos los empleados y usuarios externos a la fiesta la información y procesamiento de información de instalaciones deberán ser retirados a la terminación de su empleo, contrato o acuerdo, o ajustado en el cambio.
	A.9.4	**A.9.4.2**	Cuando se requiera la política de control de acceso, el acceso a los sistemas y aplicaciones serán controlados por un procedimiento de conexión segura.

		A.9.4.3	Sistemas de gestión de contraseñas deberán ser interactivo y deberá asegurar contraseñas de calidad.
		A.9.4.4	El uso de programas de utilidad que podría ser capaz de anular controles del sistema y de las aplicaciones que tendrán carácter reservado y fuertemente revisado.
	A.10.1	**A.10.1.1**	Una política sobre el uso de controles criptográficos para la protección de información deberá ser desarrollado e implementado.
		A.10.1.2	Una política sobre el uso, la protección y la duración de las claves de cifrado será desarrollado e implementado a través de todo su ciclo de vida**.**
	A.12.1	**A.12.1.1**	Los procedimientos de operación deberán ser documentados y puestos a disposición todos los

			usuarios que lo necesiten.
		A.12.1.2	Los cambios en la organización, los procesos de negocios, procesamiento de la información y sistemas que afectan a la seguridad de información deberán ser controlados.
		A.12.1.3	El uso de los recursos será supervisado, se ajusta y proyecta hechos futuros como requisito de capacidad para asegurar que el sistema requerido tome acción.
		A.12.1.4	Entornos de desarrollo, prueba y operativos estarán separados para reducir el riesgo de acceso no autorizado o cambios en el entorno operativo.
	A.12.3	**A.12.3.1**	Copias de seguridad de la información, software y de imágenes del sistema serán tomados y analizados periódicamente de

			acuerdo con una copia de seguridad acordado con la política.
	A.12.4	**A.12.4.1**	Los registros de eventos registrarán las actividades del usuario, excepciones, fallas e información de los eventos de seguridad que se producen, atienden y son regularmente revisados.
		A.12.4.2	Registro de instalaciones e información debe ser protegido contra manipulación y acceso no autorizado.
		A.12.4.3	El administrador del sistema y operador del sistema serán encargarán de almacenar y proteger los registros protegidos y revisarlos con regularidad.
	A.12.6	**A.12.6.1**	Información acerca de las vulnerabilidades técnicas de los sistemas de información será utilizada en el

			momento oportuno, la organización expondrá vulnerabilidades evaluadas y medidas apropiadas adoptadas para abordar el riesgo asociado.
	A.12.7	**A.12.7.1**	Los requisitos de auditoría y las actividades relacionadas con la verificación de funcionamiento de los sistemas deberán ser cuidadosamente planificados y acordados para reducir al mínimo interrupciones en los procesos de negocio.
	A.13.1	**A.13.1.1**	Las redes deberán ser gestionadas y controladas para proteger la información en los sistemas y aplicaciones.
		A.13.1.2	Los mecanismos de seguridad, niveles de servicio y los requisitos de gestión de todos los servicios de red serán identificados e incluidos en acuerdos de servicios de red, si

			estos servicios se proporcionan en la empresa o son subcontratados.
		A.13.1.3	Grupos de servicios de información, usuarios y sistemas de información deberá estar separado en las redes.
	A.14.2	**A.14.2.2**	Los cambios en los sistemas dentro del ciclo de desarrollo deben ser controlados por el uso de procedimientos formales de control de cambios.
		A.14.2.5	Se establecerán principios para sistemas seguros de ingeniería, documentado, mantenido y aplicado a cualquier sistema de información que requiera implementación.
		A.14.2.6	Las organizaciones deberán establecer y proteger adecuadamente entornos de desarrollo para el desarrollo e

			integración de sistemas que cubren todo el ciclo de vida de desarrollo del sistema.
	A.14.3	**A.14.3.1**	Los datos de prueba deben seleccionarse cuidadosamente, protegidos y controlados.
	A.15.1	**A.15.1.1**	Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso del proveedor de bienes de la organización serán acordados con el proveedor y documentado.
		A.15.1.3	Acuerdos con proveedores incluirán los requisitos para hacer frente a los riesgos de seguridad asociados con la información.
	A.16.1	**A.16.1.2**	Los eventos de seguridad de la información deben ser reportados a través de canales apropiados de gestión lo más rápidamente posible.

	A.16.1.3	Los empleados y contratistas que utilizan información de la organización y sistemas requerirán notificación y reporte de cualquier observación o debilidades en la seguridad de la información de sistemas o servicios.
	A.16.1.6	Los conocimientos adquiridos a partir del análisis y la solución de incidentes de seguridad de la información pueden utilizarse para reducir la probabilidad o el impacto de incidentes en el futuro.
	A.16.1.7	La organización debe definir y aplicar procedimientos para la identificación, colección, adquisición y conservación de la información, que puede servir como prueba.

	A.17.1	**A.17.1.1**	La organización debe determinar sus necesidades de seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas , por ejemplo, durante una crisis o desastre
	A.17.2	**A.17.2.1**	Información de las instalaciones de procesamiento se llevará a cabo con redundancia suficiente para satisfacer los requisitos de disponibilidad.
	A.18.1	**A.18.1.3**	Los registros deben ser protegidos de la pérdida, destrucción, falsificación, el acceso no autorizado y la liberación no autorizada, de acuerdo con los requisitos contractuales y comerciales.
		A.18.1.5	Controles criptográficos se utilizarán de acuerdo con toda la información

			pertinente acuerdos, leyes y reglamentos.
	A.18.2	**A.18.2.1**	El enfoque de la organización para la gestión de seguridad de la información y su puesta en marcha (es decir, objetivos de control, controles, políticas, procesos, revisando los procedimientos de seguridad de la información) independientemente a intervalos planificados o cuando ocurren cambios significativos
		A.18.2.2	Los gestores deberán comprobar periódicamente el cumplimiento del procesamiento la información dentro de su área de responsabilidad con las políticas de seguridad, las normas y cualquier otro requisito.
		A.18.2.3	Los sistemas de información deben ser revisados regularmente por el cumplimiento con las políticas y estándares de

			seguridad de la información de la organización.
Medios de Comunicación o entrega de información	**A.5.1**	**A.5.1.1**	Un conjunto de políticas de seguridad de la información se definirá, este será aprobado por un flujo de autorización, publicado y comunicado a los empleados y partes externas relevantes.
	A.6.1	**A.6.1.1**	Todas las responsabilidades de seguridad de la información deben estar definidos y asignados.
	A.7.2	**A.7.2.1**	Se deberá exigir que todos los empleados y contratistas para aplicar seguridad de la información de acuerdo con las políticas establecidas y procedimientos de la organización.
		A.7.2.2	Todos los empleados de la organización y, en su caso, los contratistas deberán recibir educación adecuada y la formación de la

			conciencia y actualizaciones regulares en las políticas y procedimientos de la organización, como relevante para su función de trabajo.
	A.8.3	**A.8.3.3**	Los medios que contienen información estarán protegidos contra acceso no autorizado, uso indebido o corrupción durante el transporte.
	A.9.2	**A.9.2.1**	Un proceso de registro de usuarios y de registro formal será implementado para permitir la asignación de derechos de acceso.
		A.9.2.2	Un proceso de provisión de acceso de usuario oficial se llevará a cabo a asignar o revocar los derechos de acceso para todos los tipos de usuario a todos los sistemas y servicios.
		A.9.2.3	La asignación y utilización de los derechos de acceso preferentemente

			deberá ser restringido y controlado.
	A.9.4	**A.9.4.2**	Cuando lo requiera la política de control de acceso, el acceso a los sistemas y aplicaciones serán controlados por un procedimiento de conexión segura.
	A.11.1	**A.11.1.5**	Procedimientos para trabajar en las áreas de seguridad deberán diseñarse y ser aplicadas.
		A.11.1.6	Los puntos de acceso, tales como áreas de entrega y de carga y otros puntos donde las personas no autorizadas puedan entrar en los locales serán controlados, y si es posible, aislarlo de procesamiento de la información para evitar el acceso no autorizado.
	A.12.1	**A.12.1.1**	Los procedimientos de operación deberán ser documentados y puestos a disposición todos los usuarios que lo necesiten.

	A.12.4	**A.12.4.1**	Los registros de eventos registrarán las actividades del usuario, excepciones, fallas e información de los eventos de seguridad que se producen, atienden y son regularmente revisados.
	A.12.6	**A.12.6.1**	Información acerca de las vulnerabilidades técnicas de los sistemas de información será utilizada en el momento oportuno, la organización expondrá vulnerabilidades evaluadas y medidas apropiadas adoptadas para abordar el riesgo asociado.
	A.12.7	**A.12.7.1**	Los requisitos de auditoría y las actividades relacionadas con la verificación de funcionamiento de los sistemas deberán ser cuidadosamente planificados y acordados para reducir al mínimo

			interrupciones en los procesos de negocio.
	A.13.1	**A.13.1.1**	Las redes deberán ser gestionadas y controladas para proteger la información en los sistemas y aplicaciones.
		A.13.1.2	Los mecanismos de seguridad, niveles de servicio y los requisitos de gestión de todos los servicios de red serán identificados e incluidos en acuerdos de servicios de red, si estos servicios se proporcionan en la empresa o son subcontratados.
		A.13.1.3	Grupos de servicios de información, usuarios y sistemas de información deberá estar separado en las redes.
	A.13.2	**A.13.2.1**	Transferencia de políticas de manera formal, procedimientos y controles adecuados en aquellos lugares para proteger la transferencia de

			información mediante el uso de todos los tipos de servicios de comunicación.
		A.13.2.2	Los contratos deberán dirigirse a la transferencia segura de información comercial entre la organización y las partes externas.
		A.13.2.3	Información involucrada en la mensajería electrónica estará debidamente protegido.
		A.13.2.4	Los requisitos para los acuerdos de confidencialidad o de no divulgación lo que refleja las necesidades de la organización para la protección de la información deberán ser identificadas, revisado y documentados con regularidad.
	A.14.1	**A.14.1.1**	Los requisitos relacionados con la seguridad de la información se incluirán en los requisitos para los nuevos sistemas de

			información o mejoras de los sistemas de información existentes.
		A.14.1.2	Información involucrada en los servicios de aplicación que pasen sobre redes públicas deberán estar protegidos de la actividad fraudulenta, disputa contractual de una revelación no autorizada y la modificación.
	A.16.1	**A.16.1.2**	Los eventos de seguridad de la información deben ser reportados a través de canales apropiados de gestión lo más rápidamente posible.
		A.16.1.3	Los empleados y contratistas que utilizan información de la organización y sistemas requerirán notificación y reporte de cualquier observación o debilidades en la seguridad de la información de sistemas o servicios.

	A.17.1	**A.17.1.1**	La organización debe determinar sus necesidades de seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre
	A.18.2	**A.18.2.2**	Los gestores deberán comprobar periódicamente el cumplimiento del procesamiento la información dentro de su área de responsabilidad con las políticas de seguridad, las normas y cualquier otro requisito.
		A.18.2.3	Los sistemas de información deben ser revisados regularmente por el cumplimiento con las políticas y estándares de seguridad de la información de la organización.

Anexo 2:

Código criptográfico desarrollo en Transact SQL utilizado para cifrar la información sensible entregada para la implementación del esquema de seguridad.

```
--Crear una columna en la que almacene los datos cifrados.

ALTER TABLE [BI].[dbo].[DB_SALESCREDIT]

ADD CardNumber_EncryptedbyPassphrase varbinary(256);


DECLARE @PassphraseEnteredByUser nvarchar (128);

SET @PassphraseEnteredByUser

   = '9$xvdl@|YII9O17';


-- Actualizar el registro de la tarjeta de crédito del usuario.

-- En este caso, el registro es el número 3681.

UPDATE[BI].[dbo].[DB_SALESCREDIT1]

SET CardNumber_EncryptedbyPassphrase = EncryptByPassPhrase(@PassphraseEnteredByUser  cc, id, ssn)


-- Obtenga la contraseña del usuario

DECLARE @PassphraseEnteredByUser nvarchar(128);

SET @PassphraseEnteredByUser   = '9$xvdl@|YII9O17';


-- Descifrar el registro cifrado.

SELECT CC, CardNumber_EncryptedbyPassphrase AS 'Encrypted card number', CONVERT (nvarchar, DecryptByPassphrase (@PassphraseEnteredByUser, CardNumber_EncryptedbyPassphrase, id, CONVERT (varbinary, ssn))) AS 'Decrypted card number' FROM  BI.[dbo].[DB_SALESCREDIT1]
```

```
CREATE ASYMMETRIC KEY AsymKey_BI
WITH ALGORITHM = RSA_2048
ENCRYPTION BY PASSWORD = 'rPs0B/m1xZP4[8_'
--Creando un algoritmo con algoritmo simetrico
CREATE ASYMMETRIC KEY AsymKey_BI
WITH ALGORITHM = RSA_2048
ENCRYPTION BY PASSWORD = 'rPs0B/m1xZP4[8_'

--Nos ayuda a cambiar la contraseña de nuestro algoritmo
ALTER ASYMMETRIC KEY AsymKey_BI
WITH PRIVATE KEY ( DECRYPTION BY PASSWORD = 'rPs0B/m1xZP4[8_',
ENCRYPTION BY PASSWORD = 'rPs0B/m1xZP4[9_');
--Para poder eliminar la contraseña de nuestro algoritmo se debe crear una Master Key
CREATE MASTER KEY ENCRYPTION BY PASSWORD = '23384923987hxJ#KLe';
--Se procede a remover la contraseña de cifrado
ALTER ASYMMETRIC KEY AsymKey_BI WITH PRIVATE KEY (
DECRYPTION BY PASSWORD = 'rPs0B/m1xZP4[9_' );

SELECT  *
FROM    sys.configurations
ORDER BY name ;
GO
```

```
-- Ahora se utilizará CertProperty para analizarlo

-- Propiedades

DECLARE @CertSubject sql_variant;

set @CertSubject = CertProperty( Cert_ID('CertInicial'), 'Subject');

PRINT CONVERT(nvarchar, @CertSubject);

GO


--Creación de un certificado autofirmado, protegido mediante una contraseña

CREATE CERTIFICATE TC_SalesCreditC

ENCRYPTION BY PASSWORD = 'pGFD4bbefdjkd3300387y'  --Clave inicial

WITH SUBJECT = 'Tesis_Test',   --Tema

EXPIRY_DATE = '20401031';  --Fecha de vencimiento

GO


CREATE CERTIFICATE TC_SalesCredit

WITH SUBJECT = 'Tesis_Test',

GO


--Cambio de contraseña de certificado

ALTER CERTIFICATE  TC_SalesCreditC

WITH PRIVATE KEY (DECRYPTION BY PASSWORD = 'ewjewkewm#39siw', --
Clave inicial

ENCRYPTION BY PASSWORD = '4329578#340dkw');  --Nueva Clave

GO
```

```
ALTER CERTIFICATE TC_SalesCreditC

WITH PRIVATE KEY (ENCRYPTION BY PASSWORD = 'ewjewkewm#39siw',  -- Nueva Clave

DECRYPTION BY PASSWORD = '4329578thlkajdshglXCSgf');  ---Clave Nueva

GO


SELECT Cert_ID('TC_SalesCreditC');

GO


-- Inserta datos encriptados de la base por de la clave asimétrica

INSERT INTO DB_SALESCREDITCIPHER (CC, Cipher)

SELECT a.cc, EncryptByAsymKey(AsymKey_ID('SecureAsymmetricKey'), a.cc) from BI.DBO.DB_SALESCREDIT1 A


SELECT CC, CONVERT(NVARCHAR(100), DecryptByAsymKey(AsymKey_ID('SecureAsymmetricKey'), Cipher,N'QWWOEWODLMSD')) AS PlainText

FROM DB_SALESCREDITCIPHER;


--Backup de certificado que tiene una clave preestablecida

BACKUP CERTIFICATE TC_SalesCreditC TO FILE = 'c:\keys\tcsalescreditcert'

WITH PRIVATE KEY ( DECRYPTION BY PASSWORD = 'pGFD4bbefdjkd3300387y'
,

 FILE = 'c:\keys\tcsalescreditkey' ,
```

```
 ENCRYPTION BY PASSWORD = '4329578thlkajdshglXCSgf' );
GO

--Crear algoritmo simétrico utilizando un certificado preestablecido
CREATE SYMMETRIC KEY SymKey01
WITH ALGORITHM = AES_256
ENCRYPTION BY CERTIFICATE TC_SalesCreditC;

-- Crear una columna en donde se cifrará la información
ALTER TABLE [dbo].[DB_SALESCREDIT1]
ADD EncryptedCreditNumber varbinary(128);

-Se modificado el certificado para poder abrirlo con el algoritmo simétrico
ALTER CERTIFICATE TC_SalesCreditC
WITH PRIVATE KEY (DECRYPTION BY PASSWORD = 'pGFD4bbefdjkd3300387y');

--Abrir el algoritmo simétrico con el cual está cifrada la información
OPEN SYMMETRIC KEY SymKey01
DECRYPTION BY CERTIFICATE TC_SalesCreditC;

--Una vez abierto el algoritmo simetrico, se procede a ejecutar la actualización
UPDATE [BI].[dbo].[DB_SALESCREDIT1]
SET [EncryptedCreditNumber]= EncryptByKey(Key_GUID('SymKey01'),cc);
```

```
--Visualización de información

SELECT cc, [EncryptedCreditNumber]

   AS 'Encrypted ID Number',

   CONVERT(nvarchar, DecryptByKey([EncryptedCreditNumber]))

   AS 'Decrypted ID Number'

   FROM [BI].[dbo].[DB_SALESCREDIT1]


--Mostrar propiedades extendidas en una base de datos

--En el ejemplo siguiente se comprueba si la tabla spt_fallback_db de la base de datos maestra está firmada

--por el certificado de firma de esquema.

USE master;

-- Declare a variable to hold a thumbprint and an object name

DECLARE @thumbprint varbinary(20), @objectname sysname;


-- Populate the thumbprint variable with the thumbprint of

-- the master database schema signing certificate

SELECT @thumbprint = thumbprint

FROM sys.certificates

WHERE name LIKE '%SchemaSigningCertificate%';

-- Populate the object name variable with a table name in master

SELECT @objectname = 'spt_fallback_db';

-- Query to see if the table is signed by the thumbprint

SELECT @objectname AS [object name],
```

```
IS_OBJECTSIGNED(

'OBJECT', OBJECT_ID(@objectname), 'certificate', @thumbprint

) AS [Is the object signed?] ;


---Visualización del nombre de una clave simétrica mediante key_guid

DECLARE @guid uniqueidentifier ;

SELECT @guid = key_guid FROM sys.symmetric_keys

WHERE name = '##MS_DatabaseMasterKey##' ;

-- Demonstration of passing a GUID to KEY_NAME to receive a name

SELECT KEY_NAME(@guid) AS Nombre_algoritmo;
```

Anexo 3:
Código realizado en la evaluación de la información para el incremento de ingresos de la compañía.

1) Análsis correspondiente al mes de agosto (realizado de la misma forma para los meses anteriores)

```
SELECT DISTINCT  [Fecha_Transaccion]
    ,[Tipo_Transaccion]
    ,[Cod_Cliente]
    ,[Cod_Transaccion]
    ,[Fecha_Proc_Transaccion]
    ,[Monto_Transaccion]
    ,[Cuenta_Cliente]
    ,[Fecha_Transaccion_Comi]
    ,[Tipo_TransaccionComi]
    ,[Cod_ClienteComi]
    ,[Cod_TransaccionAsociado]
    ,[Fecha_Proceso_Comi]
    ,[Monto_TransaccionComi]
    ,[CuentaComiAsociado]
        ,Contratado = CASE WHEN B.[Tip_Sobregiro] IS NOT NULL THEN 'X'
ELSE NULL END
        ,B.[Monto_Excedio] Excedio_OK
        ,B.Monto_Sobregiro
```

```
        ,Corto_Plazo = CASE WHEN C.[Tip_Sobregiro] IS NOT NULL THEN 'X'
ELSE NULL END
        ,C.Valor_Asignado
        ,D.Estatus
        ,D.Disponible Monto_Diario
        INTO CHEQUES.DBO.ANALISIS_AGOSTO
  FROM [DIARIOS].[dbo].[COMISIONES_AGOSTO] A
  LEFT JOIN DIARIOS.[dbo].[DIARIOS_SOBREGIRO_CONTRATADO_AGOSTO]
B ON A.[Cuenta_Cliente] = B.Cuenta_ClienteBDContratado AND A.Cod_Cliente =
B.Codigo_ClienteBDContratado
  AND A.[Fecha_Transaccion] = B.Fecha
  LEFT JOIN DIARIOS.[dbo].[DIARIOS_SOBREGIRO_CORTOPLAZO_AGOSTO]
C ON A.[Cuenta_Cliente] = C.Cuenta
  LEFT JOIN CHEQUES.DBO.DIARIO_AGOSTO D ON A.Fecha_Transaccion =
D.Fecha AND A.Cuenta_Cliente = D.Cuenta
  WHERE A.[Cod_Cliente] <> 0 AND A.[Cuenta_Cliente] <> 0
```

2) Manejo de la información para visualizar la inversión de los clientes en sobregiro contratado

```
SELECT  [Cuenta]
     ,[Anio]
    , Mes = CASE WHEN Mes <= 9 THEN +'0'+Mes Else Mes END,
          Dia = CASE WHEN Dia <= 9 THEN +'0'+Dia Else Dia END
     ,[Estatus]
    ,SUM(Disponible) OVER(PARTITION BY Cuenta) AS 'Disponible'
   ,SUM(Libros) OVER(PARTITION BY Cuenta) AS 'Libros'
        ,B.LNEAMN
        ,Estatus_Monto = CASE WHEN B.LNEAMN > Libros THEN 'Excedio' Else
'No Excedio' End
        INTO Saldos_Diarios_Excedio
  FROM [F_CHEQUES].[dbo].[SaldosDiarios] A
  LEFT JOIN  CHEQUES.DBO.[SOBRE_CONTRATADO]  B ON A.Cuenta =
B.LNEADN
  ORDER BY B.LNEAMN, Cuenta, Dia
```

Anexo 3:
GLOSARIO

ISO/IEC 27001: Es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.

ISO/IEC 27018: Es un código de buenas prácticas en controles de protección de datos para servicios de computación en la nube. La norma se complementa con la norma ISO 27001 e ISO 27002 en el ámbito de gestión de la seguridad de la información y que se dirige de forma específica a los proveedores de servicios de nube.

SGSI: Sistema de Gestión de Seguridad de la Información, según ISO 27001 consiste en preservar la confidencialidad, integridad y disponibilidad, además de todos los sistemas implicados en el tratamiento dentro de la organización.

ISMS: Information security management system

CPS: Contenido de protección y seguridad

ISAE: Norma Internacional sobre compromisos de aseguramiento

SOC: Son informes de análisis independientes de terceros que demuestran de qué manera en que la nube o servidor logra los controles y objetivos clave de conformidad. La finalidad de estos informes es ayudarle a usted y a sus auditores a entender los controles que se han establecido como soporte a las operaciones y la conformidad.

HIPAA: Es la Ley de Responsabilidad y Transferibilidad de Seguros Médicos (Health Insurance Portability and Accountability Act) promulgada por el Congreso y decretada en agosto de 1996.

AICPA: Instituto Americano de contadores públicos certificados

CDSA: Content Delivery & Security Association

BSI: British Standard Institution

SLA: Service Level Agreement es un acuerdo escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio.

IDC: International Data Corporation

IDG: International Data Group

AWS: Amazon Web Services es una colección de servicios de computación en la nube (también llamados servicios web) que en conjunto forman una plataforma de computación en la nube, ofrecidas a través de Internet por Amazon.com.

NIST: Instituto Nacional de Normas y Tecnología, llamada entre 1901 y 1988 Oficina Nacional de Normas, es una agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos.

Amazon EC2: Es un servicio web que proporciona capacidad informática en la nube segura y de tamaño modificable.

Amazon S3: Ayuda realizando Backup y Archive, Big Data y mucho más.

DBaaS: Base de datos como servicio, es un servicio de pago por uso que permite el acceso bajo demanda a una base de datos. Este tipo de servicio es atractivo para los clientes, ya que estos se libran de los costes y las cargas del despliegue y el mantenimiento del hardware y el software, que corre a cargo de los proveedores.

RDBMS: Sistema de gestión de bases de datos relacionales, es un programa que te permite crear, actualizar y administrar una base de datos relacional.

NBS: National Bureau of Standards (Agencia Nacional de Normalización)

PDCA: Plan-Do-Check-Act o Ciclo Deming es un método iterativo de gestión de cuatro pasos utilizado en los negocios para el control y la mejora continua de procesos y productos.

Redundancia: Es el proceso mediante el que los archivos son almacenados en diferentes lugares una vez que entran en el sistema. Es decir, los archivos son copiados al menos en dos lugares al mismo tiempo.

VPN: Es una tecnología de red de computadoras que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet.

BigQuery: Es un servicio web RESTful que permite el análisis interactivo de grandes conjuntos de datos que trabajan en conjunto con Google Storage. Es una Infraestructura como servicio público (IaaS) que puede utilizarse de forma complementaria con MapReduce.

Amazon VPC: Amazon Virtual Private Cloud (Amazon VPC) le permite lanzar recursos de AWS en una red virtual definida por el usuario. Dicha red virtual es prácticamente idéntica a las redes tradicionales que se utilizan en sus propios centros de datos, con los beneficios que supone utilizar la infraestructura escalable de AWS.

TLS: Transport Layer Security es una evolución del protocolo SSL (Secure Sockets Layer), es un protocolo mediante el cual se establece una conexión segura por medio de un canal cifrado entre el cliente y servidor.

NSA: National Security Agency

Amazon Redshift: Amazon Redshift, el servicio de almacén de datos rentable, sencillo y rápido de AWS.

Amazon WAF: Es un firewall de aplicaciones web que ayuda a proteger sus aplicaciones web de vulnerabilidades web comunes que podrían afectar la disponibilidad de las aplicaciones, comprometer la seguridad o consumir recursos excesivos.

EBS: Fue el primer sistema de comercio que ofreció soporte para sistemas algorítmicos de trading en el mercado forex "ocultos" (black box) a través de su API (Application Programming Interface).

API: Application Programming Interface, es un conjunto de subrutinas, funciones y procedimientos (o métodos, en la programación orientada a objetos) que ofrece cierta biblioteca para ser utilizado por otro software como una capa de abstracción.

IDEA: International Data Encryption Algorithm

SSL: Secure Sockets Layer es un protocolo diseñado para permitir que las aplicaciones para transmitir información de ida y de manera segura hacia atrás.

WEP: Wired Equivalent Privacy

TDE: Transparent Data Encryption

HSM dispositivos: "Hardware Security Module" (Módulo de Seguridad Hardware). Un HSM es un dispositivo criptográfico basado en hardware que genera, almacena y protege claves criptográficas y suele aportar aceleración hardware para operaciones criptográficas.

ETL: Extract, Transform and Load es el proceso que permite a las organizaciones mover datos desde múltiples fuentes, reformatearlos y limpiarlos, y cargarlos en otra base de datos, datamart, o data warehouse para analizar, o en otro sistema operacional para apoyar un proceso de negocio.

Azure Data Factory: Le ayuda a crear, programar, supervisar y administrar canalizaciones de datos. Una canalización de datos se compone de actividades que pueden mover datos entre almacenes de datos locales y en la nube, pero también transforma datos para generar información en la que se pueda confiar.

EKM: Extensible Key Management

SHA: Secure Hash Algorithm